(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－53794
（P2001－53794A）
(43)公開日　平成13年２月23日(2001.2.23)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｈ０４Ｌ　12/56		Ｈ０４Ｌ　11/20	１０２Ａ	５Ｋ０１４
1/22		1/22		５Ｋ０３０
12/28		11/20	Ｃ	５Ｋ０３５
29/14		13/00	３１１	

審査請求　有　請求項の数11　ＯＬ　（全 11 頁）

(21)出願番号　特願平11－224868

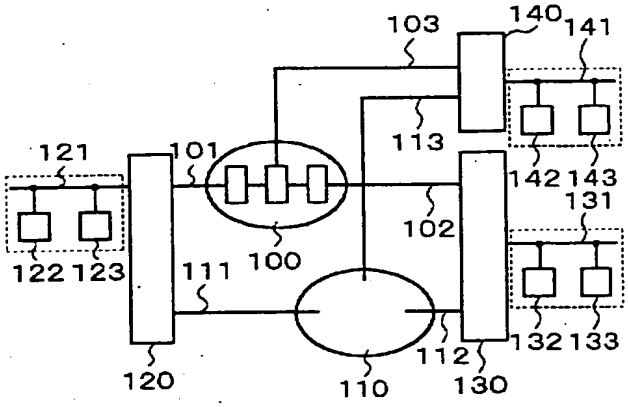
(22)出願日　平成11年８月９日(1999.8.9)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　鈴木　光男
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100102864
弁理士　工藤　実　（外１名）

Ｆターム(参考)　5K014 CA06
5K030 GA12 HC01 HC14 HD07 LB08 MB01 MD02
5K035 AA03 AA04 BB03 BB04 LL17

(54)【発明の名称】　ＩＰ通信のリアルタイムバックアップ通信方法

(57)【要約】
【課題】　経済的であるインターネット網の網障害、網遅延時間による通信品質の低下を安価に、且つ、簡略に回避する。
【解決手段】　送信側ノード１２０と受信側ノード１３０との間を接続するＩＰ網１００の上のリアルタイム通信中のリアルタイム通信の障害の発生を検出して、リアルタイム通信の通信呼を送信側ノード１３０と受信側ノード１２０との間で自動的に公衆網１１０へ迂回させる。このような迂回により、リアルタイム通信を継続することができる。障害発生は、リアルタイム通信の品質を確保できない程度の遅延時間の発生である。周期的送受信には、ＩＣＭＰが用いられる。リアルタイム通信の途中に新たなリアルタイム通信呼が発生することがある。そのような場合、その新たなリアルタイム通信も公衆網１１０上に迂回させられて、そのリアルタイム通信が可能になる。その障害が回復した場合は、リアルタイム通信は、公衆網からＩＰ網に戻される。



【特許請求の範囲】
【請求項1】送信側ノードと受信側ノードとの間を接続するIP網の上のリアルタイム通信中のリアルタイム通信の障害の発生を検出すること、
前記検出に基づいて、前記リアルタイム通信の通信呼を前記送信側ノードと前記受信側ノードとの間で自動的に公衆網へ迂回させることとからなるIP通信のリアルタイムバックアップ通信方法。
【請求項2】請求項1において、
前記発生は、前記リアルタイム通信の品質を確保できない程度の遅延時間の発生であるIP通信のリアルタイムバックアップ通信方法。
【請求項3】請求項2において、
前記周期的送受信にはICMPが用いられるIP通信のリアルタイムバックアップ通信方法。
【請求項4】請求項2において、更に、
前記リアルタイム通信の途中に新たなリアルタイム通信呼が発生した場合、前記新たなリアルタイム通信を前記公衆網に迂回させることとからなるIP通信のリアルタイムバックアップ通信方法。
【請求項5】請求項2において、更に、
前記迂回の間、前記送信側ノードと前記受信側ノードとの間を接続する前記公衆網上のリアルタイム通信の障害の発生を検出することからなるIP通信のリアルタイムバックアップ通信方法。
【請求項6】請求項5において、更に、
前記迂回の間の前記公衆網上の前記検出は、前記送信側ノードと前記受信側ノードとの間のエコー要求メッセージとエコー応答メッセージの周期的送受信の時間を検出することを含むIP通信のリアルタイムバックアップ通信方法。
【請求項7】請求項6において、更に、
前記迂回の間の前記検出は、前記公衆網上に前記障害が発生している間に前記エコー要求メッセージが正常に受信された場合は、前記公衆網は正常であり前記ノードが異常であると判断することを含むIP通信のリアルタイムバックアップ通信方法。
【請求項8】請求項2において、更に、
前記検出は、前記送信側ノードと前記受信側ノードとの間のエコー要求メッセージとエコー応答メッセージの周期的送受信の時間を検出することを含むIP通信のリアルタイムバックアップ通信方法。
【請求項9】請求項8において、更に、
前記検出は、前記エコー応答メッセージが正常に返信された場合、前記IP網に障害がなく、且つ、前記ノードに障害があると判断することを含むIP通信のリアルタイムバックアップ通信方法。
【請求項10】請求項2において、更に、
前記IP網上のリアルタイム通信の障害の回復を検出すること、
前記回復の検出に基づいて、前記リアルタイム通信の通信呼を前記公衆網上から前記IP上へ復帰させることとからなるIP通信のリアルタイムバックアップ通信方法。
【請求項11】請求項10において、
前記IP上の前記障害の回復を検出することと前記公衆網上のリアルタイム通信の障害の発生を検出することとから、前記ノードの障害と前記IP網の障害とを判別することからなるIP通信のリアルタイムバックアップ通信方法。
【発明の詳細な説明】
【0001】
【発明の属する技術分野】本発明は、IP通信のリアルタイムバックアップ通信方法に関し、特に、公衆網を利用するIP通信のリアルタイムバックアップ通信方法に関する。
【0002】
【従来の技術】近年、インターネット、イントラネット、エキストラネット（これらは、以下、インターネット網又はIP網といわれる）上の音声、動画のようなデータは、リアルタイム通信が行われ始めている。そのリアルタイム通信の品質をできるだけ保証するためのQoS（品質保証）制御に関して、IETF標準化の活動が活発になってきており、以下に、その主なものが記述される。
1．RSVP（ReSource reserVation Protocol ）：資源予約プロトコル
2．RTP/RTCP（Real-time Transport Protocol）／（Real-time Transport Control Protocol）：リアルタイム通信制御プロトコル
3．DiffServe（Differentiated Services）：IPヘッダを用いた優先制御
4．RTSP（Real-time Transport Streaming Protocol）：リアルタイム・ストリームデータ制御プロトコル
【0003】これらのQoS制御は、これのみでは、インターネット網上で安定したリアルタイム通信を行うことは不可能であり、例えば、インターネット網に接続されるノードの障害、網障害により送信側ノードからの音声データ、動画データなどのリアルタイム通信呼が受信側ノードでエラーを発生することになる：再送制御を行わないUDP（User Datagram Protocol）手順での通信形態であるリアルタイム通信は、インターネット網障害をノード側で検出する手段がなく、その障害が対向ノード障害であるか、網障害であるか、どちらであるかを区別することができない。
【0004】このような現状では、ユーザーからの通信異常申告によって始めて網障害を検知する高度な能力を有する保守技術者は、ノード間にエコー要求メッセージを送出し、エコー応答メッセージの返信がないことによって始めて異常を確認し、その技術者が手動によりIN

Ｓ等の公衆網に切り替えてバックアップ切り替えを行う方法をとっている。このような方法の実行に必要な障害原因の特定のためには、技術者の高度な保守技術が必要であり、更に、そのような高度の保守技術者は、網障害、通信障害の特定を行うための多くの工数を必要としていた。更に、ユーザー申請から、高度保守技術者による手動操作に関わる一連の障害解析による時間が多くかかり、その間の著しいサービスの低下を招いている。

【０００５】特に、近年のＩＰネットワークによる網のダウンサイジング化、フラット（水平）化にともない、企業内に多く存在する小規模網ごとに、専門的であり、且つ、高度である保守技術を配置することは経済的にも困難であり、低級な一般業務との兼任保守兼務者すなわち各部門でアサインされた素人の保守者でも速やかに障害原因を特定できる仕組みが必要とされ始めてきている。言い換えれば、低信頼、低品質であるが非常に経済的であるインターネット網の網障害、網遅延時間による通信品質の低下を安価な方法によりユーザー機器側で監視して、リアルタイム通信呼の安定かつ継続的な通信をおこなうことができるＩＰ網の信頼性を経済的に確保する構成を確立することの要望が大きくなってきている。

【０００６】

【発明が解決しようとする課題】本発明の課題は、非常に経済的であるインターネット網の網障害、網遅延時間による通信品質の低下を安価に、且つ、簡略に回避することができるＩＰ通信のリアルタイムバックアップ通信方法を提供することにある。本発明の他の課題は、リアルタイム通信を安定的に、且つ、継続的に実行することによりインターネット網の信頼性を経済的に確保する技術を確立することができるＩＰ通信のリアルタイムバックアップ通信方法を提供することにある。

【０００７】

【課題を解決するための手段】その課題を解決するための手段が、下記のように表現される。その表現中に現れる技術的事項には、括弧（）つきで、番号、記号等が添記されている。その番号、記号等は、本発明の実施の複数・形態又は複数の実施例のうちの少なくとも１つの実施の形態又は複数の実施例を構成する技術的事項、特に、その実施の形態又は実施例に対応する図面に表現されている技術的事項に付せられている参照番号、参照記号等に一致している。このような参照番号、参照記号は、請求項記載の技術的事項と実施の形態又は実施例の技術的事項との対応・橋渡しを明確にしている。このような対応・橋渡しは、請求項記載の技術的事項が実施の形態又は実施例の技術的事項に限定されて解釈されることを意味しない。

【０００８】本発明によるＩＰ通信のリアルタイムバックアップ通信方法は、送信側ノード（１２０）と受信側ノード（１３０）との間を接続するＩＰ網（１００）の上のリアルタイム通信中のリアルタイム通信の障害の発生を検出すること、その検出に基づいて、リアルタイム通信の通信呼を送信側ノード（１２０）と受信側ノード（１３０）との間で自動的に公衆網（１１０）へ迂回させることとからなる。このような迂回により、リアルタイム通信を継続することができる。その発生は、前記リアルタイム通信の品質を確保できない程度の遅延時間の発生である。周期的送受信には、ＩＣＭＰが用いられる。

【０００９】リアルタイム通信の途中に新たなリアルタイム通信呼が発生することがある。そのような場合、その新たなリアルタイム通信も公衆網（１１０）上に迂回させられて、そのリアルタイム通信が可能になる。その障害が回復した場合は、リアルタイム通信は、公衆網からＩＰ網に戻される。

【００１０】公衆網にも障害が発生することがある。迂回の間、送信側ノードと受信側ノードとの間を接続する公衆網上のリアルタイム通信の障害の発生が検出される。その検出は、送信側ノード（１２０）と受信側ノード（１３０）との間のエコー要求メッセージとエコー応答メッセージの周期的送受信の時間の検出によって実行される。その迂回の間の検出は、公衆網（１１０）上に障害が発生している間にエコー要求メッセージが正常に受信された場合は、公衆網（１１０）は正常でありノード（１２０又は１３０）が異常であると判断する。

【００１１】ＩＰ網（又は、単にＩＰ）（１００）上のその検出は、送信側ノード（１２０）と受信側ノード（１３０）との間のエコー要求メッセージとエコー応答メッセージの周期的送受信の時間を検出することにより実行される。その検出は、エコー応答メッセージが正常に返信された場合、ＩＰ網（１００）に障害がなく、且つ、ノード（１２０又は１３０）に障害があると判断する。一般的には、ＩＰ（１００）上の障害の回復を検出することと、公衆網（１１０）上のリアルタイム通信の障害の発生を検出することとから、ノード（１２０，１３０）の障害とＩＰ網（１００）の障の判別を行うことができる。

【００１２】

【発明の実施の形態】図に一致対応して、本発明によるＩＰ通信のリアルタイムバックアップ通信方法の実施の形態は、公衆（回線）網１１０がＩＰ（インタネット網）１００とともに設けられている。そのＩＰ１００には、図１に示されるように、ＩＰ側第１接続インタフェース１０１を介して、送信側ノード１２０が接続している。ＩＰ１００は、ＩＰ側第２接続インタフェース１０２とＩＰ側第３接続インタフェース１０３を介して、受信側第１ノード１３０と受信側第２ノード１４０にそれぞれに接続している。

【００１３】その公衆網１１０には、公衆網側第１接続インタフェース１１１を介して、送信側ノード１２０が接続している。公衆網１１０は、公衆網側第２接続イン

タフェース１１２と公衆網側第３接続インタフェース１１３を介して、受信側第１ノード１３０と受信側第２ノード１４０にそれぞれに接続している。

【００１４】送信側音声端末１２２と送信側動画端末１２３は、送信側ＬＡＮ１２１に接続している。送信側ＬＡＮ１２１は、送信側ノード１２０に接続している。第１受信側音声端末１３２と第１受信側動画端末１３３は、第１受信側ＬＡＮ１３１に接続している。受信側ＬＡＮ１３１は、受信側第１ノード１３０に接続している。第２受信側音声端末１４２と第２受信側動画端末１４３は、第２受信側ＬＡＮ１４１に接続している。第２受信側ＬＡＮ１３１は、受信側第２ノード１４０に接続している。

【００１５】音声、動画のようなデータを送受信するマルチメディア通信であるリアルタイム通信では、通信誤りが発生した時に、メッセージの再送によって遅延を引き起こす＊プロトコル（図５参照）が”１６進の６”であるＴＣＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｒｏｌ Ｐｒｏｔｏｃｏｌ）を用いず、誤りが発生しても再送を行わない＊プロトコルビットが”１６進の１７”であるＵＤＰ（ＵｓｅｒＤａｔａｇｒａｍ Ｐｒｏｔｏｃｏｌ）が用いられる。

【００１６】ＬＡＮ１２１に接続された音声端末１２２と動画端末１２３は、図２に示される「ＩＥＥＥ ８０２．１ＱのＴａｇ付きＥｔｈｅｒｎｅｔフレーム」で構成される。リアルタイム性が高い音声、動画は、この規定のＴａｇの内の３ビットのＵｓｅｒ Ｐｒｉｏｒｉｔｙにより最も優先度の高い値に設定されている。

【００１７】ＩＰ１００は、リアルタイム性が高い音声、動画のために、ＱｏＳ（帯域保証）が可能な制御（例示：ネットワーク層（ＩＰ）を補間する形式のシグナリング制御）として使用され、情報を受信する受信側の主導により単方向にネットワーク資源を予約するためのプロトコルとして図３に示されるＲＳＶＰ（ＲｅＳｏｕｒｃｅ ｒｅｓｅｒＶａｔｉｏｎ Ｐｒｏｔｏｃｏｌ：資源予約プロトコル）、更には、ユーザとＩＳＰ（Ｉｎｔｅｒｎｅｔ Ｓｅｒｖｉｃｅ Ｐｒｏｖｉｄｅｒ）との間の契約に基づく優先制御サービスであり、従来、ほとんど使用されていなかった図４に示されるＩＰヘッダ内のＴＯＳ（Ｔｙｐｅ Ｏｆ Ｓｅｒｖｉｃｅ）フィールド（８ビット長）をＤｉｆｆｅｒｅｎｔｉａｔｅｄ Ｓｅｒｖｉｃｅｓフィールドとして再定義し、その上位６ビットをＰＨＢ（Ｐｅｒ－Ｈｏｐ－Ｂｅｈａｖｉｏｒ）フィールドと名付け、その中の３ビットを用いて６段階の優先度を設定することができるＩＰヘッダを用いた優先制御であるＤｉｆｆＳｅｒｖｅ（Ｄｉｆｆｅｒｅｎｔｉａｔｅｄ Ｓｅｒｖｉｃｅｓ）、その他（ＩＰ ｏｖｅｒ）のＡＴＭにおけるＱｏＳ設定などの制御が可能な構成となっている。

【００１８】ＩＰ１００には、更に、網には依存せずに端末間、すなわち トランスポート層、アプリケーション間でのリアルタイム通信品質を向上させるために、送信側端末からのヘッダにメッセージ毎の物理時刻情報やシーケンス番号を付与することにより、受信側で再生速度の制御、メディア間の同期制御をおこなうリアルタイム通信制御プロトコルであるＲＴＰ／ＲＴＣＰ（Ｒｅａｌ-ｔｉｍｅ Ｔｒａｎｓｐｏｒｔ Ｐｒｏｔｏｃｏｌ）／（Ｒｅａｌ-ｔｉｍｅ Ｔｒａｎｓｐｏｒｔ Ｃｏｎｔｒｏｌ Ｐｒｏｔｏｃｏｌ）、及び、受信側から秒当たりの動画フレーム数や解像度などの表示品質、通信速度などを動的に送信側に伝えるストリームデータ制御プロトコルであるＲＴＳＰ（Ｒｅａｌ-ｔｉｍｅ ＴｒａｎｓｐｏｒｔＳｔｒｅａｍｉｎｇ Ｐｒｏｔｏｃｏｌ）が搭載されて設けられている。

【００１９】ＬＡＮ１２１上の送信側音声端末１２２と第１受信側ＬＡＮ１３１上の第１受信側音声端末１３２との間で、ＩＰ１００を介してリアルタイム電話通信を行う場合が、次に考えられる。送信側音声端末１２２は、図２に示される「ＩＥＥＥ８０２．１Ｑ Ｔａｇ付きＥｔｈｅｒｎｅｔフレーム」に第１受信側音声端末１３２に相当するＤＡ（Ｄｅｓｔｉｎａｔｉｏｎ Ａｄｄｒｅｓｓ）を設定し、且つ、そのＴａｇの中のＵｓｅｒ Ｐｒｉｏｒｉｔｙ に最優先ビットを設定して、送信側ノード１２０上に送出する。

【００２０】送信側ノード１２０は、送信側ＬＡＮ１２１上のＤＡ（Ｄｅｓｔｉｎａｔｉｏｎ Ａｄｄｒｅｓｓ）から第１受信側音声端末１３２に相当するＩＰ番号（受信側第１ノード１３０のＩＰ番号）に変換すると同時に、Ｕｓｅｒ Ｐｒｉｏｒｉｔｙの最優先ビットを検出し、ＩＰ１００のＱｏＳ制御［ＲＳＶＰ、ＤｉｆｆＳｅｒｖｅ または、（ＩＰ ｏｖｅｒ）ＡＴＭのＱｏＳ］にマッピングする。

【００２１】ここでは、送信側ノード１２０が、ＱｏＳ制御として、図４のＤｉｆｆＳｅｒｖｅにおけるＩＰヘッダのＰＨＢ（Ｐｅｒ－Ｈｏｐ－Ｂｅｈａｖｉｏｒ）フィールドの中の３ビットに最優先ビットを設定してＩＰ網に送出する場合が１例として説明されている。その結果、図１に示されるように、送信側音声端末１２２－送信側ＬＡＮ１２１－送信側ノード１２０－ＩＰ側第１接続インタフェース１０１－ＩＰ１００－ＩＰ側第２接続インタフェース１０２－受信側第１ノード１３０までのＱｏＳを確保したリアルタイム通信を確保することができ、更に、受信側第１ノード１３０は内部ＬＡＮ１３１から第１受信側音声端末１３２までを、図２の「８０２．１Ｑ Ｔａｇ付きＥｔｈｅｒｎｅｔフレーム」に第１受信側音声端末１３２に相当するＤＡ（Ｄｅｓｔｉｎａｔｉｏｎ Ａｄｄｒｅｓｓ）及びＴａｇ内にＵｓｅｒ Ｐｒｉｏｒｉｔｙ に最優先ビットを設定して送出することにより、送信側音声端末１２２と第１受信側音声端末１３２の間をＩＰ１００を介したＱｏＳ制御によるリ

アルタイム通信が可能となる。

【0022】図5の＊プロトコルの8ビットが16進の1である場合には、図6及び図7のICMP（Internet Control Message Protocol）の指定となり、タイプ（メッセージタイプ）の8ビットが"16進の8"の場合にはエコー要求、それが"0"の場合にはエコー応答をあらわす。これらの要求・応答の実行の際、IP100に接続されているホストやノードが生きているかどうかを確認するときにエコー機能が用いられている。このために、あるホスト又はノードがメッセージタイプ8のエコー要求を送ると、指定されたホストやノードは、応答できる状態であれば、メッセージタイプ0のエコー応答を送り返す。このようなエコーによる動作確認は頻繁に行われるものであり、一般にはピング（ping）と呼ばれるユーティリティプログラムがエコー要求を送り出す。

【0023】送信側ノード120は、図8に示されるように、図5に示される送信元アドレスに送信側ノード120のIPアドレス番号を設定し、宛先アドレスにノード130のIPアドレス番号を設定し、＊プロトコルに16進の1（ICMP）を設定し、更に、図7に示されるメッセージタイプに16進の8（図6のエコー要求）を設定し、図7のデータ（可変長）にループバック用テストデータを設定した図8のエコー要求メッセージ800をIP100を介して、受信側第1ノード130に送出する。

【0024】受信側第1ノード130が、図8のエコー要求メッセージ800を受信すると、図5の送信元アドレスに受信側第1ノード130のIPアドレス番号を設定し、宛先アドレスに送信側ノード120のIPアドレス番号を設定し、＊プロトコルに16進の1（ICMP）を設定し、更に、図7のメッセージタイプには16進の0（図6のエコー応答）を設定、図7のデータ（可変長）に受信した図8のエコー要求メッセージ800のデータフィールドに書き込まれているループバック用テストデータをそのままコピーして、図8のエコー応答メッセージ801として送信側ノード120に送り返すことにより、送信元ノードである送信側ノード120はループバックテストにより、データ授受の状況を確認することができ、送信側ノード120－IP側第1接続インタフェース101－IP100－IP側第2接続インタフェース102－受信側第1ノード130の経路での網及びノードの障害を検出することができると同時に、ノード120がエコー要求メッセージ800を送出してから、受信側第1ノード130から送り返されるエコー応答メッセージ801が受信されるまでの一巡時間（ラウンドトリップタイム）がリアルタイム通信品質を確保できる時間以内であるか、例えば、ITU－TG．114で規定する150msec以内であれば、良好なリアルタイム電話通信品質を確保できていることを確認することができる。

【0025】このような前提条件の下で、図1の送信側音声端末122が送信側LAN121、送信側ノード120、IP側第1接続インタフェース101、IP100、IP側第2接続インタフェース102、受信側第1ノード130、第1受信側LAN131を介して第1受信側音声端末132の間でリアルタイム通信を行う場合、送信側LAN121から到来する図2のTag付きEthernetフレームを送信側ノード120で受信し、このTag内のUser PriorityによりQoSの最優先検出を行い、DA（Destination Address）から第1受信側音声端末132へのIPアドレス番号への変換が行われる。

【0026】同時に、図10のAに示されるように送信側LAN121から送信側ノード120に到来する音声データパケットにより、図10のBに示される音声データパケット断検出用のタイムオーバーカウンタをクリアして、音声通信中モード（Lレベル）にする。以降、送信側LAN121から送信側ノード120に、リアルタイム通信を確保するために引き続き一定時間以内には、必ず到来する音声データパケット毎に、図10のBに示される音声データパケット断検出用のタイムオーバーカウンタをクリアして、音声通信中モード（Lレベル）を継続する。

【0027】音声通信の終了に伴って、図10のBに示される音声データパケット検出用のタイムオーバーカウンタのクリア信号が到来しなくなるので、当該カウンタはタイムオーバーによりHレベルの無通話モードになる。送信側ノード120はQoS制御として図4に示されるDiffServeにおけるIPヘッダのPHB（Per－Hop－Behavior）フィールドの中の3ビットに最優先ビットを設定し、図5の＊プロトコルに16進の17（UDP：User Datagram Protocol）を設定し、送信元アドレスに送信側音声端末122を収容する送信側ノード120のIPアドレス番号を設定し、宛先アドレスに第1受信側音声端末132を収容する受信側第1ノード130のIPアドレス番号を設定して、図2のIEEE802．1Q Tag付きEthernetフレームのペイロードにある音声データを図9のトランスポート層のUDPのデータ（可変部）にコピーし、IP100を介して、受信側第1ノード130に送出する。受信側第1ノード130はこの受信した音声データを図9のUDPの宛先ポート番号即ちアプリケーション、図4のIPヘッダ内のPHB（Per－Hop－Behavior）内の3ビットの優先ビットにより、リアルタイム通信呼すなわちQoS制御の要求呼を検出し、第1受信側LAN131上に図2のIEEE802．1Q Tag付きEthernetフレーム内にUser Priorityに最優先ビットを設定して、第1受信側音声端末132に送出

する。この結果、送信側音声端末１２２と第１受信側音声端末１３２との間でのＱｏＳを保証したリアルタイム通信が可能となる。

【００２８】同時に、送信側ノード１２０はＱｏＳ制御として、図4のＤｉｆｆＳｅｒｖｅにおけるＩＰヘッダのＰＨＢ（Ｐｅｒ－Ｈｏｐ－Ｂｅｈａｖｉｏｒ）フィールドの中の3ビットに最優先ビットを設定し、図5の＊プロトコルに１６進の１（ＩＣＭＰ：Ｉｎｔｅｒｎｅｔ Ｃｏｎｔｒｏｌ Ｍｅｓｓａｇｅ Ｐｒｏｔｏｃｏｌ）を設定し、送信元アドレスに送信側音声端末１２２のＩＰアドレス番号を設定し、宛先アドレスに第1受信側音声端末１３２のＩＰアドレス番号（受信側第１ノード１３０のＩＰアドレス番号）を設定し、図7のメッセージタイプに１６進の８（エコー要求）を設定し、データ（可変長）にループバック用テストデータを設定した図8のエコー要求メッセージ８００をＩＰ１００を介して受信側第１ノード１３０に送出する。

【００２９】以降、このエコー要求メッセージ８００は、図１０のＢの音声データパケット断検出用のタイムオーバーカウンタ出力がＬレベルである音声通信中モードの間に、図１０のＣの一定間隔（周期）毎に、定期的に送出される。送信側ノード１２０は、図１０のＣの一定時間以内に受信側第１ノード１３０から送り返されるエコー応答メッセージ８０１が受信されるまでの一巡時間（ラウンドトリップタイム）がリアルタイム通信品質を確保できる時間以内であるか否かを、図１０のＤのタイムオーバーカウンタで検出し、図１０のＥのようにラウンドトリップタイム経過後のエコー応答メッセージ８０１の受信、及び、図１０のＦのようにエコー応答メッセージ８０１が返信されない場合には、ＩＰ又は対向ノード１３０の障害と判断する。

【００３０】この場合、送信側ノード１２０は、接続先の第１受信側音声端末１３２のＩＰアドレス番号（受信側第１ノード１３０のＩＰアドレス番号）から、公衆網１１０の電話番号に変換してダイアルアップによる公衆網接続により、送信側ノード１２０－公衆網側第１接続インタフェース１１１－公衆網１１０－公衆網側第２接続インタフェース１１２－受信側第１ノード１３０までのバックアップ迂回ルートを確保し、送信側ノード１２０は受信側第１ノード１３０に、バックアップ切り替え迂回後の公衆網１１０を介して、図１１のエコー要求メッセージ１１００を送信して、受信側第１ノード１３０からのエコー応答メッセージ１１０１が許容時間以内に返信された場合には、ＩＰ１００が障害で受信側第１ノード１３０は正常であり、エコー応答メッセージ１１０１が返信されない場合には受信側第１ノード１３０が異常であると判別することができ、受信側第１ノード１３０の障害を検出した場合には、緊急処置を要請することができる。

【００３１】更に、このバックアップ迂回によるリアルタイム通信中は公衆網１１０通信ルートによる公衆網１１０、及び、受信側第１ノード１３０の正常性を引き続き監視するために、図８及び図１０の一連の構成による動作と全く同一の動作、即ち、エコー要求メッセージ８００を図１１のエコー要求メッセージ１１００に、エコー応答メッセージ８０１を図１１のエコー応答メッセージ１１０１に読み替えて、図１１の公衆網１１０上にも適用する構成となっている。

【００３２】同時に、送信側ノード１２０は、このＩＰ網切断／異常障害及びラウンドトリップタイムオーバーによるＩＰ内遅延時間が規定時間以上となった網輻輳状態からの正常復旧を監視するために、図１０のＢの条件の代わりに、送信側ノード１２０と受信側第１ノード１３０の間のＩＰ障害（ラウンドトリップタイムオーバーを含む）条件すなわち網障害時には強制的に図１０のＢをＬレベルにすることの条件に置き換えて、図１０のＣの一定間隔（周期）毎に、エコー要求メッセージ８００を定期的に送出する。

【００３３】送信側ノード１２０は、図8のエコー要求メッセージ８００すなわち図１０のＣに示される送出の後、一定時間以内に受信側第１ノード１３０から送り返されるエコー応答メッセージ８０１が受信されるまでの一巡時間（ラウンドトリップタイム）がリアルタイム通信品質を確保できる時間以内であるか否かを、図１０のＤのタイムオーバーカウンタで検出し、図１０のＥのようにラウンドトリップタイム許容制限時間経過後のエコー応答メッセージ８０１の受信、又は、図１０のＦのようにエコー応答メッセージ８０１が返信されない現状の障害状態から連続（安定）して正常状態に復旧するまで監視を続ける。すなわち、送信側ノード１２０と受信側第１ノード１３０の間のバックアップ迂回による通信が完了した後であっても、送信側ノード１２０と受信側第１ノード１３０間のＩＰ１００が正常状態を回復するまで、継続して監視を続けることを意味し、この間に新たに、受信側第１ノード１３０への通信呼が発生した場合には、公衆網１１０を介したバックアップ迂回を行うことになる。

【００３４】ＩＰ１００が正常安定状態を回復したことを確認した後、送信側ノード１２０から受信側第１ノード１３０までの公衆網１１０を介したリアルタイム通信が行われている場合には、この正常状態を回復したＩＰ１００に切り替えることにより、より経済的な通信を行うことができる。この場合、正常安定状態に回復したことを検出した時点で、図１０のＢのＩＰ障害条件すなわち、網障害状態である図１０のＢの強制Ｌレベル条件を一旦クリアして、イニシャル状態であるＨレベルに戻し、ＩＰへの通信呼の開始時点で、図１０のＡからの正常シーケンスによりＩＰ１００の障害監視を行う構成である。また、ＩＰ１００が正常状態に回復した時点で速やかに公衆網１１０からＩＰ１００への切り戻しを行

い、以降は、既述の一連の通常のＩＰ１００を介したリアルタイム通信を行うことは当然のことである。

【００３５】このような実施の形態では、送信側ノード１２０が発信呼側、受信側第１ノード１３０が着信呼側として記述されているが、送信側ノード１２０が着信呼側で受信側第１ノード１３０が発信呼側とした場合、送信側ノード１２０は図９のＵＤＰ（Ｕｓｅｒ　Ｄａｔａｇｒａｍ　Ｐｒｏｔｏｃｏｌ）のポート番号すなわちアプリケーション番号又は図４のＩＰヘッダ内部のＰＨＢ（Ｐｅｒ－Ｈｏｐ－Ｂｅｈａｖｉｏｒ）のＤｉｆｆＳｅｒｖｅ優先ビットの最優先設定から着信呼がリアルタイム通信呼であることを知ることができ、送信側ノード１２０が発信呼で受信側第１ノード１３０が着信呼であった図８のエコー要求メッセージ８００及びエコー応答メッセージ８０１による監視、図１０のＡ、Ｂ、Ｃ、Ｄ、Ｅ、Ｆの一連の動作、及び、図１１に関わるエコー要求メッセージ１１００およびエコー応答メッセージ１１０１の一連の動作と全く同一動作を実行することにより、ノード相互間で対称性を有するＩＰ障害、許容遅延時間を監視し、迅速な障害検出、回復保守を行うことが可能となる。

【００３６】上記は説明の容易性のために、ＩＰは、インターネット網として述べられたが、イントラネット網、エキストラネット網も包含する。ＱｏＳが保証されたＩＰにおけるリアルタイム通信について言及されているが、ＱｏＳが保証されないベストエフォートである現状の一般的なＩＰ（インターネット）網を用いて構成することが可能であり、ラウンドトリップタイムの監視により遅延時間を監視して制限時間を超えた場合に、公衆網へのバックアップ迂回を行わせることにより、より経済的なリアルタイム通信が可能である。

【００３７】また、上記の基本動作に加えて、ＩＰ（インターネット）網１００の障害発生時、及び、正常状態回復時のバックアップ切り替え、切り戻し時に発生するリアルタイム通信呼のパケットロス、遅延時間などを吸収して、より容易且つスムースなる通信安定品質を確保するために、ＭＰ（Ｔｈｅ　ＰＰＰ　Ｍｕｌｔｉｌｉｎｋ　Ｐｒｏｔｏｃｏｌ）が有益である。

【００３８】

【発明の効果】本発明によるＩＰ通信のリアルタイムバックアップ通信方法は、ＩＰ障害、及び、リアルタイム通信品質を確保できない程度の遅延時間の発生をリアルタイム通信障害として、公衆網１１０へ自動的にバックアップ切り替え迂回でき、低信頼性、低品質であるが非常に経済的なＩＰ上で、安定且つ高品質なリアルタイム通信が可能となる経済的な大きな効果に加えて、高度な保守技術者を配置することなく、低級な保守者すなわち一般業務との兼任者程度であっても保守が可能な大きな経済性と障害箇所の迅速な特定、復旧時間の短縮が可能となり、通信サービス品質向上と経済的な効果を得ることができる。

【図面の簡単な説明】

【図１】図１は、本発明によるＩＰ通信のリアルタイムバックアップ通信方法の実施の形態を示す回路ブロック図である。

【図２】図２は、Ｅｔｈｅｒｎｅｔのデータ構成図である。

【図３】図３は、ＲＳＶＰの制御方法を示すタイムチャートである。

【図４】図４は、優先制御の従来・本発明のフィールド形成を示すデータ構成図である。

【図５】図５は、ＩＰデータグラムである。

【図６】図６は、ＩＣＰＭのメッセージ表である。

【図７】図７は、ＩＣＰＭのメッセージ形成を示すデータ形成図である。

【図８】図８は、図１の一部の動作信号を示す回路ブロック図である。

【図９】図９は、ＵＤＰのメッセージ形成を示すデータ形成図である。

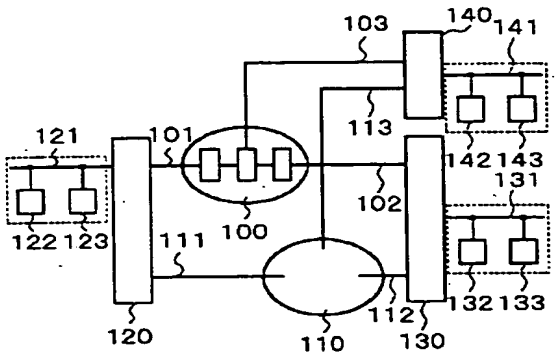
【図１０】図１０は、応答の遅延を検出する信号フローのタイミングチャートである。

【図１１】図１１は、公知装置を示す回路ブロック図である。

【符号の説明】

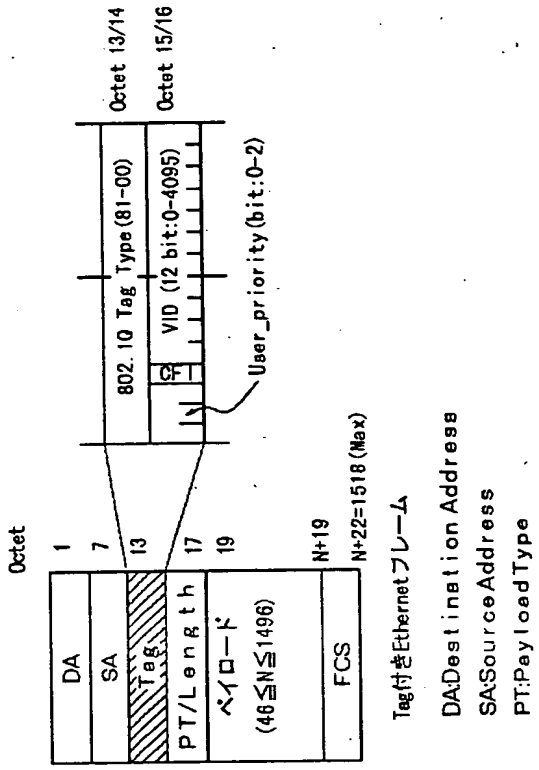
１００…ＩＰ網
１１０…公衆網
１２０…送信側ノード
１３０…受信側ノード

【図1】



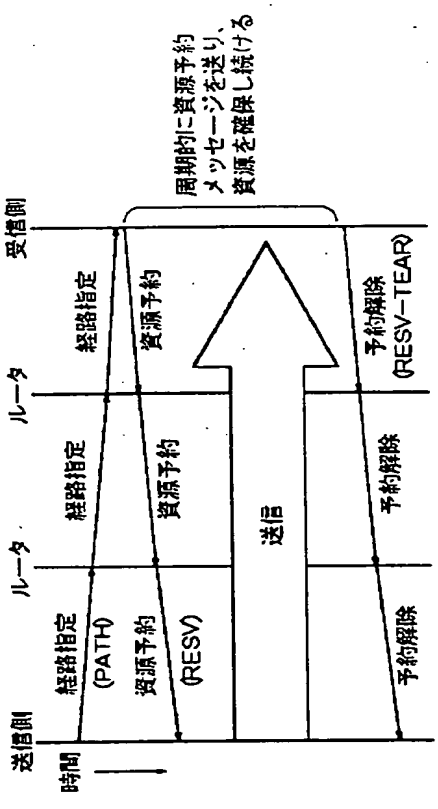
【図2】

IEEE 802.1Q Tag付きEthernetフレーム

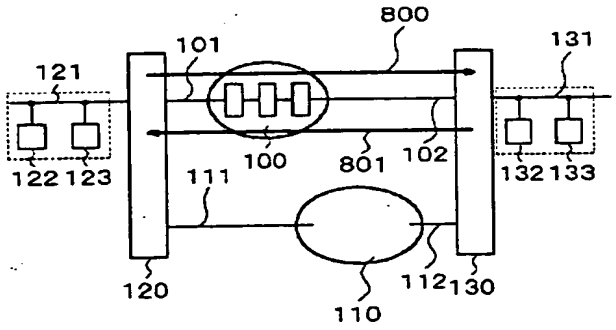


【図3】

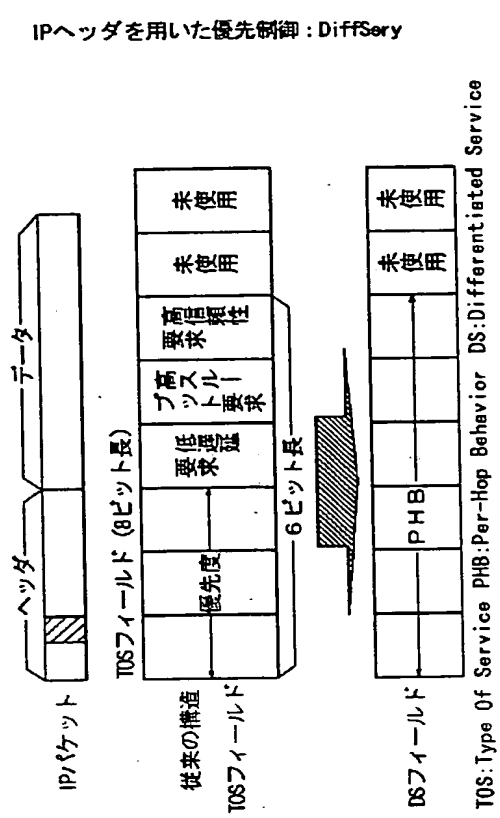
RSVPの制御手順



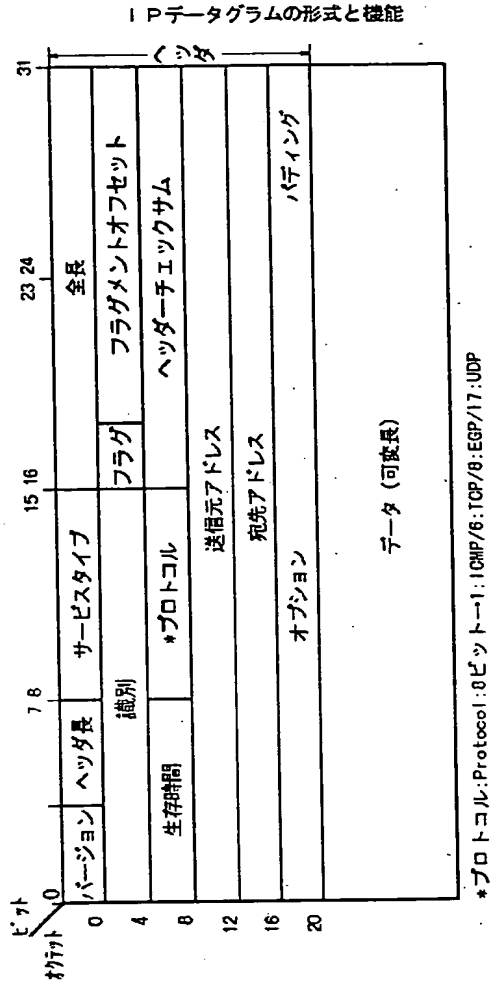
【図8】



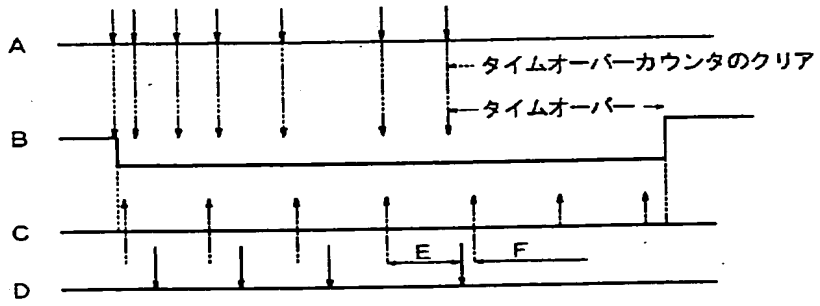
【図4】



【図5】



【図10】



A：音声端末122から音声端末132へのリアルタイム通信における音声端末122
→LAN121→ノード120への音声データパケット
B：LAN121→ノード120への音声データパケット断検出用のタイムオーバー
カウンタ出力（音声通信中がＬレベル、無通話中がＨレベル）
C：ＩＣＭＰにおける図8のエコー要求メッセージ800の送出時間範囲と送出間隔
D：C送信から図８のエコー応答メッセージ801受信までの遅延時間
E：C送信からエコー応答メッセージ801受信までの遅延が大きくタイムオーバーの場合
F：エコー応答メッセージ801が受信されずタイムオーバーの場合

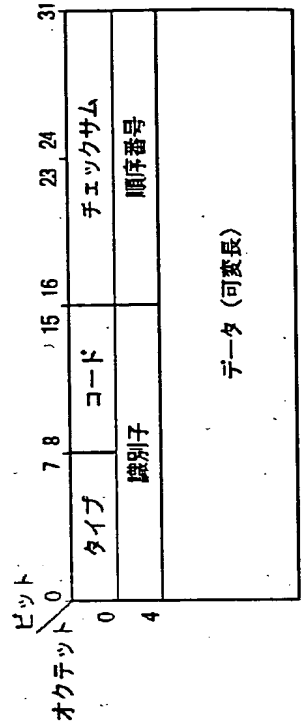
【図6】

ICMP(Internet Control Protocol)メッセージの種類

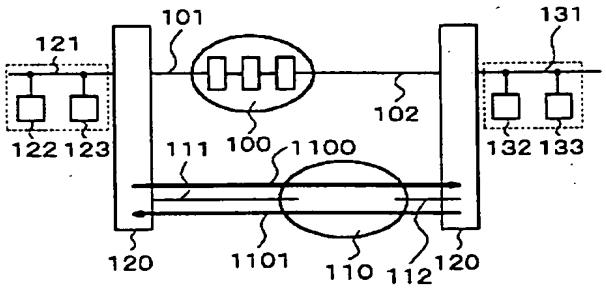
タイプ	意味	英語名
0	エコー応答	echo reply
3	宛先到達不能	destination unreachable
4	送信元抑制要求	source quench
5	経路変更要求	redirect
8	エコー要求	echo request
11	時間切れ	time exceeded
12	パラメータ異常	parameter problem
13	時刻要求	timestamp request
14	時刻応答	timestamp reply
15	情報要求	information request
16	情報応答	information reply
17	アドレスマスク要求	address mask request
18	アドレスマスク応答	address mask reply

【図7】

ICMPにおけるエコー応答とエコー要求メッセージの形式

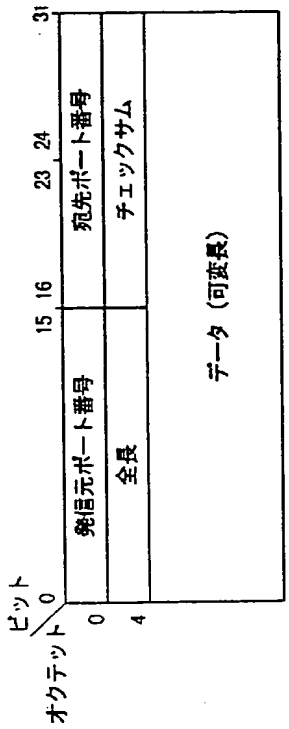


【図11】



【図9】

UDP(User Datagram Protocol)メッセージの形式



(12) UK Patent Application (19) GB (11) 2 369 019 (13) A

(43) Date of A Publication 15.05.2002

(21) Application No 0202535.1

(22) Date of Filing 09.08.2000

Date Lodged 04.02.2002

(30) Priority Data
(31) 11224868 (32) 09.08.1999 (33) JP

(62) Divided from Application No 0019611.3 under Section 15(4) of the Patents Act 1977

(51) INT CL[7]
H04M 7/00

(52) UK CL (Edition T)
H4P PEE PENE PPD
H4K KOA

(56) Documents Cited
EP 1035719 A2
EP 0920176 A2
EP 0910201 A2
WO 99/28979 A2
JP 110308345 A
US 5898668 A

(58) Field of Search
UK CL (Edition T) H4P PEE PENE PENX PEX PPD
INT CL[7] H04L 1/12 1/14 1/20 1/22 12/66 29/06, H04M 3/22 3/42 7/00
Online: WPI, EPODOC, JAPIO

(71) Applicant(s)
NEC Corporation
(Incorporated in Japan)
7-1 Shiba 5-chome, Minato-ku, Tokyo 108, Japan

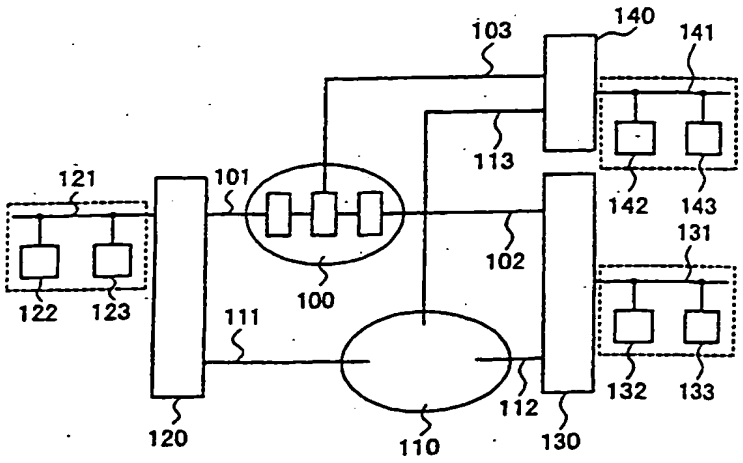
(72) Inventor(s)
Mitsuo Suzuki

(74) Agent and/or Address for Service
Mathys & Squire
100 Grays Inn Road, LONDON, WC1X 8AL,
United Kingdom

(54) Abstract Title
Method for carrying out real-time backup communication of IP communication

(57) Real-time communications are transmitted from a transmission side node 120 to a reception side node 130 via an internet protocol (IP) network 100 provided performance is deemed satisfactory. However if performance is deemed unsatisfactory the IP network is bypassed and the real-time communications are instead automatically diverted along a public network 110. If a real-time communication call is newly generated during the course of real-time communication on the public network then the newly generated real-time communication is made to go around the public network rather than the IP network. Performance is assessed by periodically transmitting echo test signals along the IP network. If the time interval between sending and receiving an echo test signal exceeds a predetermined allowed time interval then the quality of real time communication cannot be assured and performance is deemed unsatisfactory.

Fig. 1



GB 2 369 019 A

Fig. 1

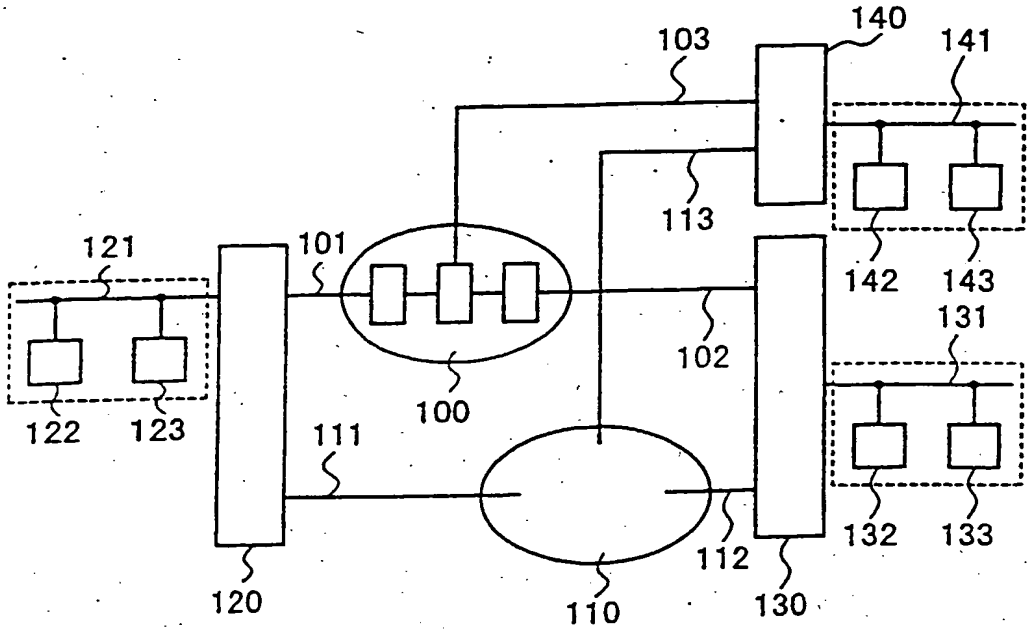


Fig. 2

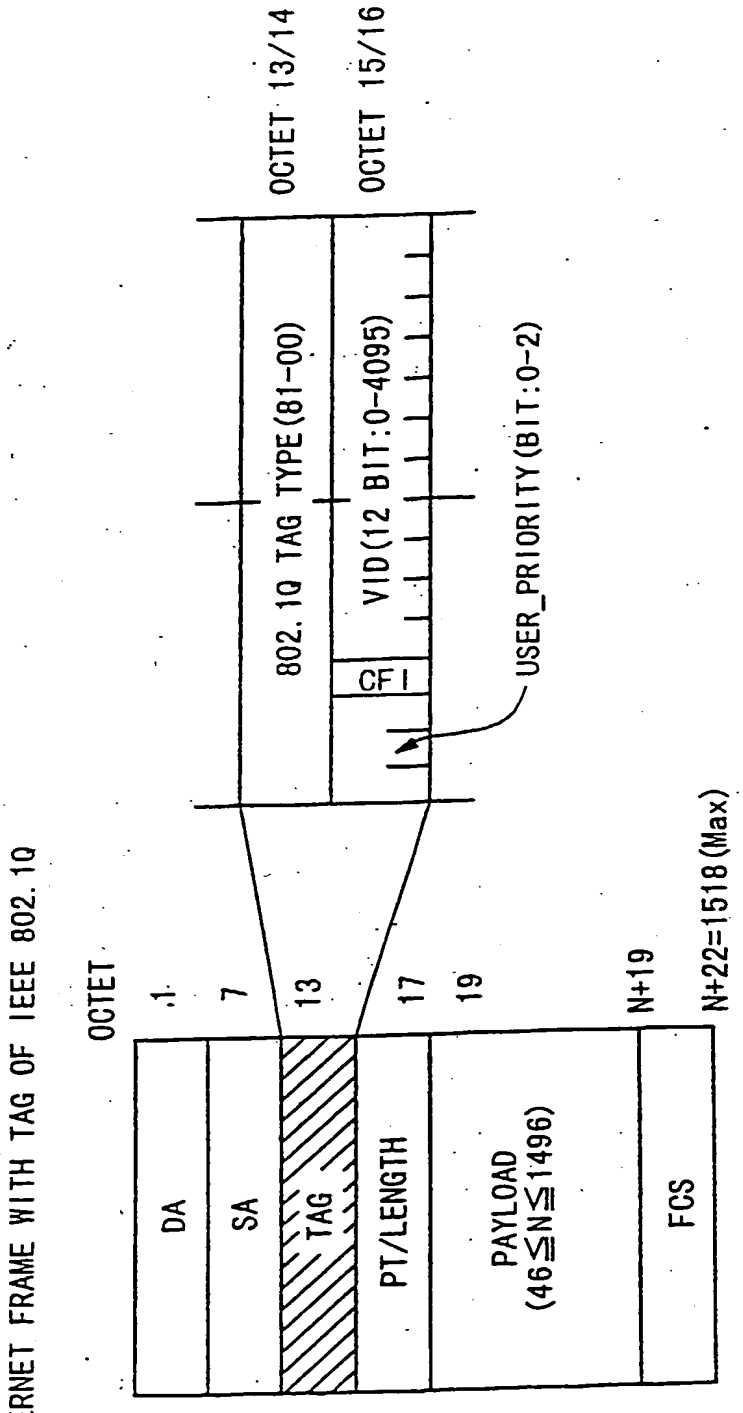


Fig. 3

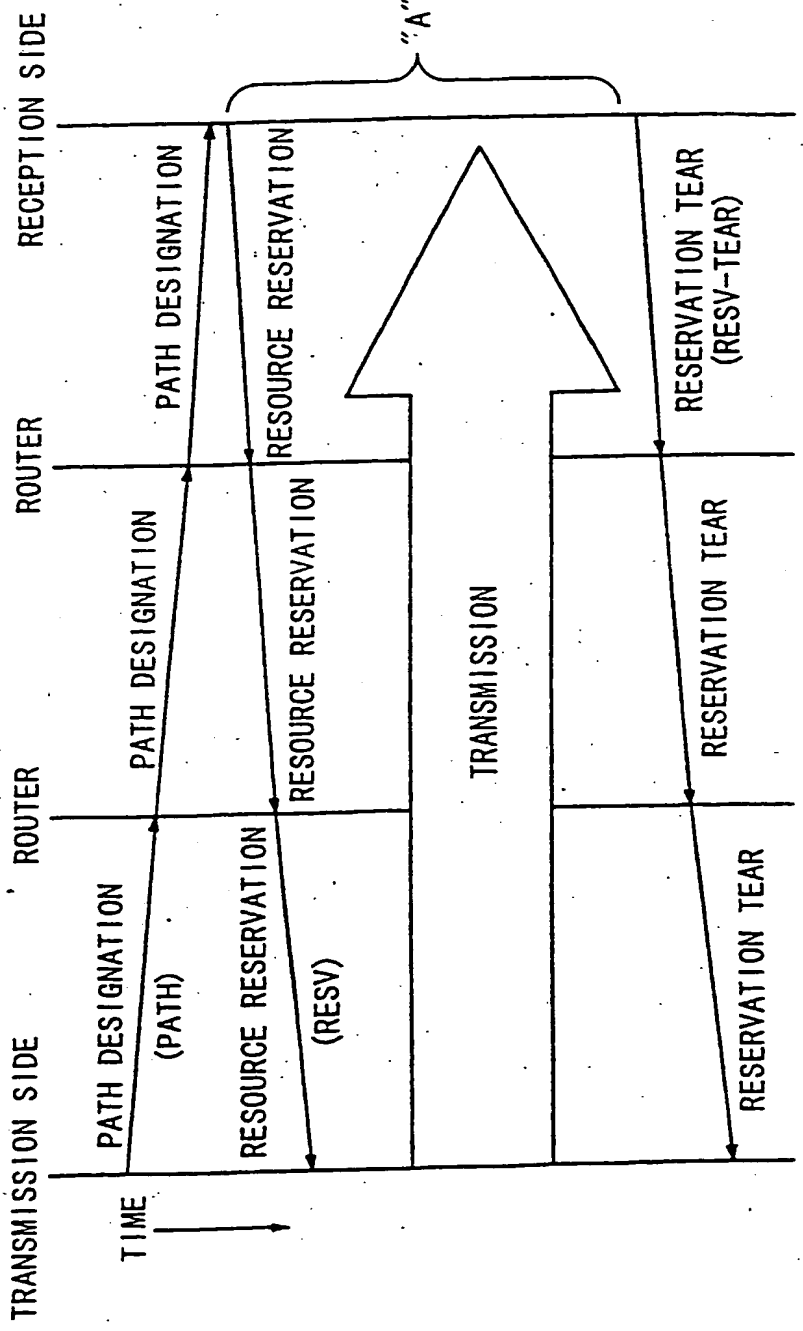


Fig. 4

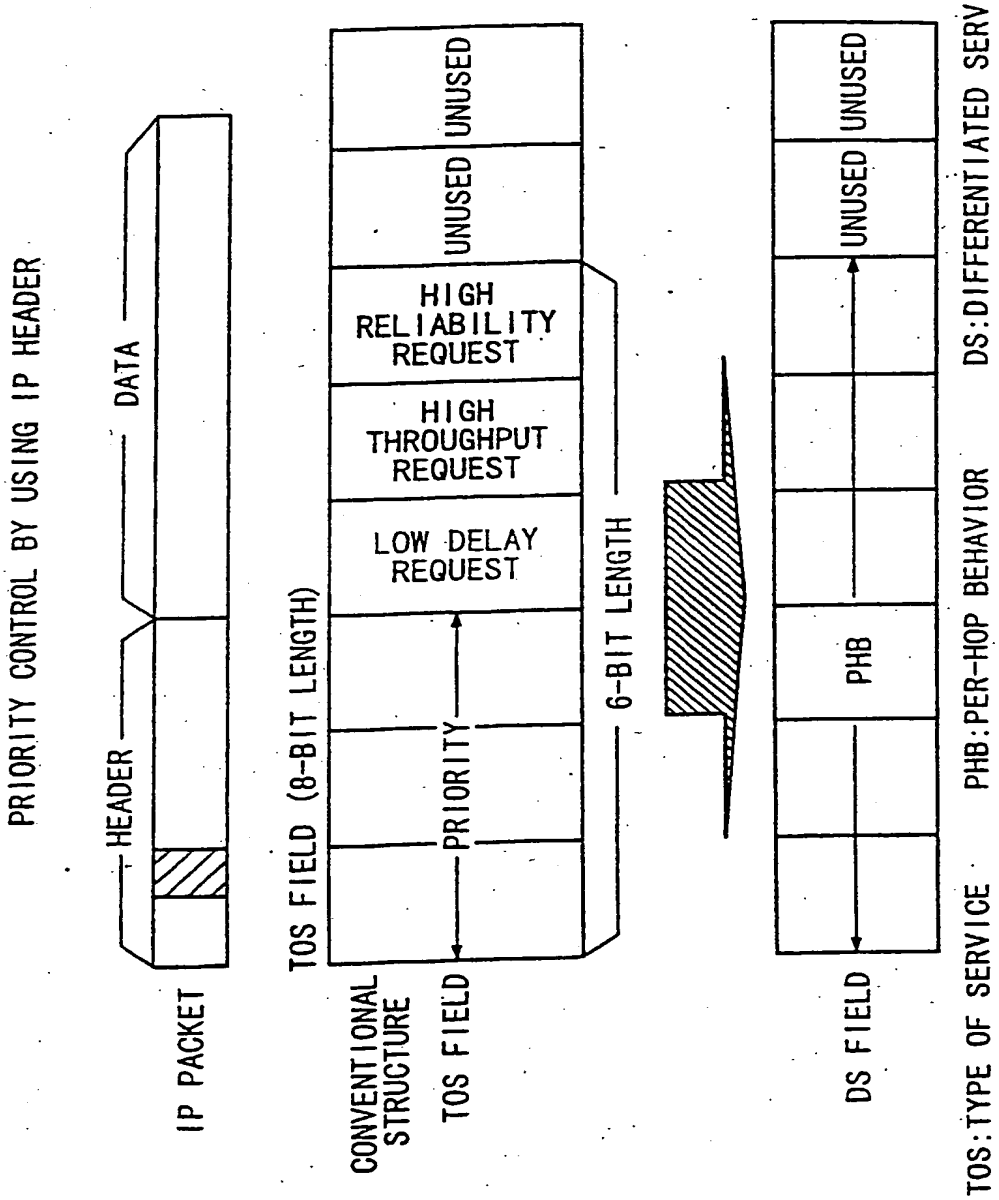


Fig. 5

IP DATAGRAM FORMAT AND FUNCTION

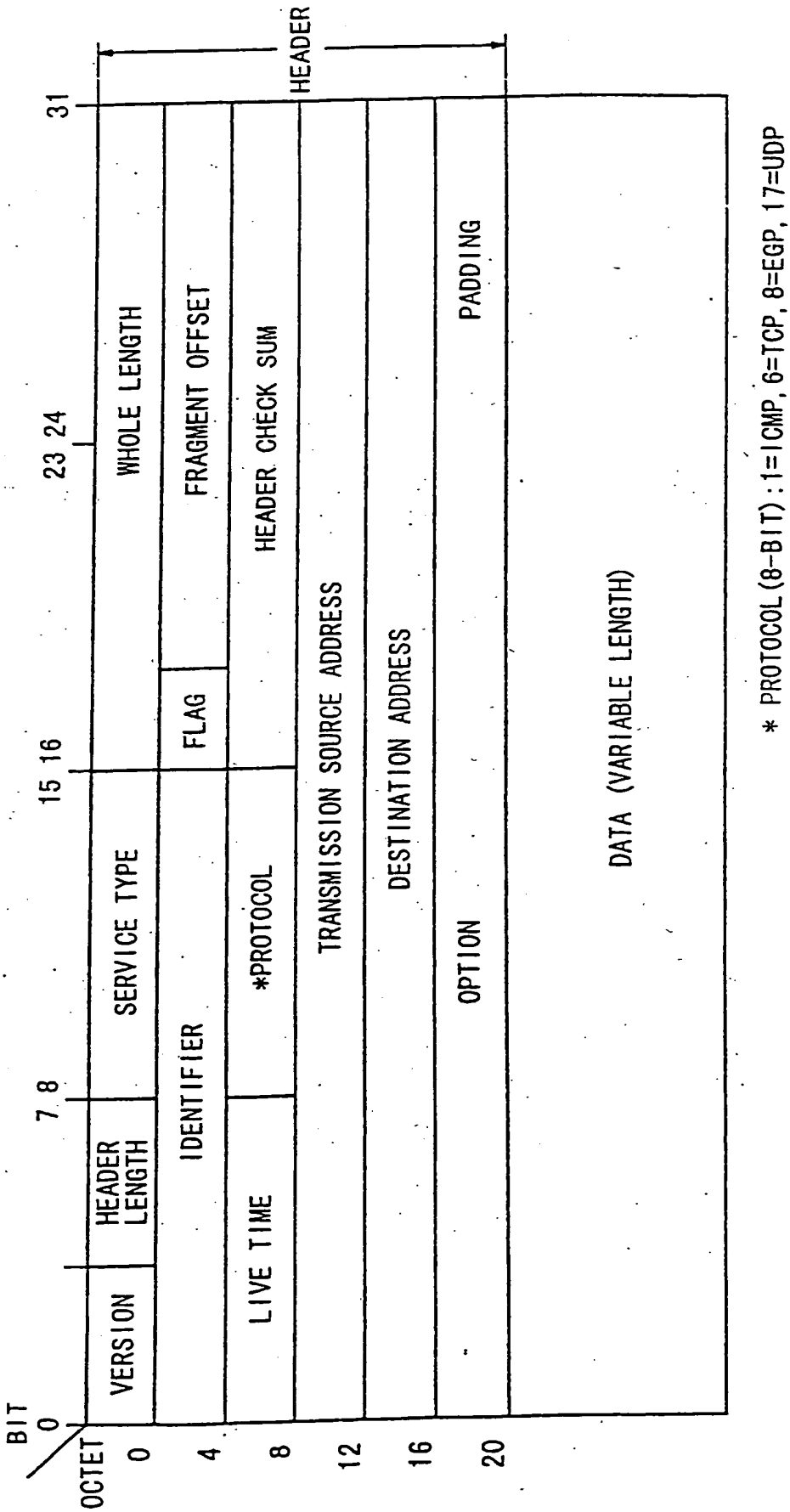


Fig. 6

KIND OF ICPM MESSAGE

TYPE	CONTENT
00	ECHO REPLY
03	DESTINATION UNREACHABLE
04	SOURCE QUENCH
05	REDIRECT
08	ECHO REQUEST
11	TIME EXCEEDED
12	PARAMETER PROBLEM
13	TIMESTAMP REQUEST
14	TIMESTAMP REPLY
15	INFORMATION REQUEST
16	INFORMATION REPLY
17	ADDRESS MASK REQUEST
18	ADDRESS MASK REPLY

Fig. 7

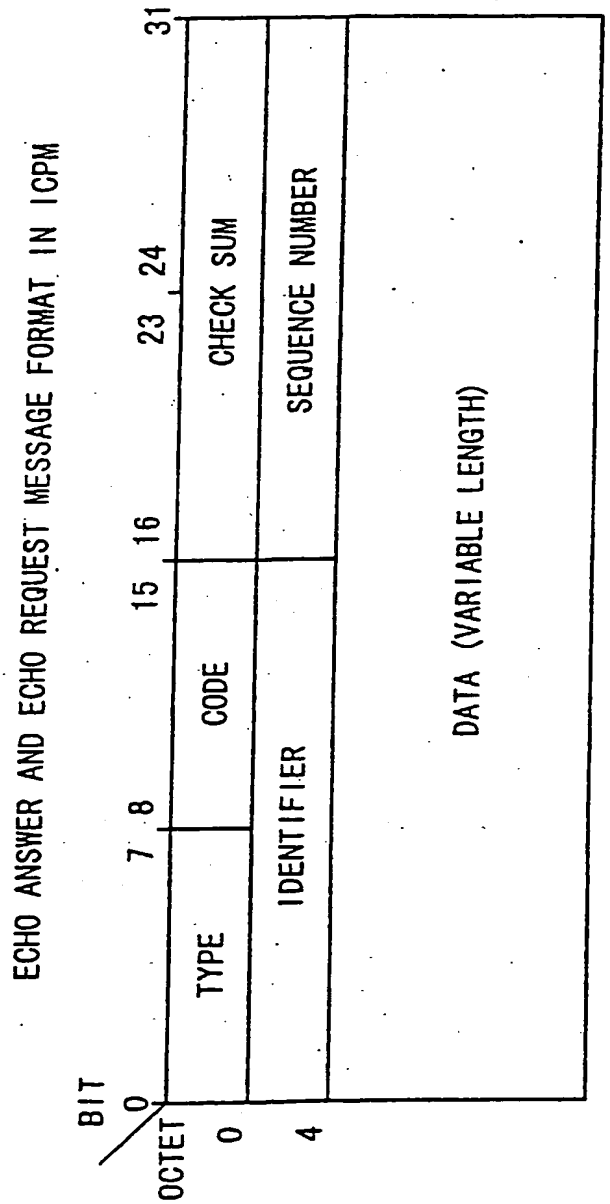


Fig. 8

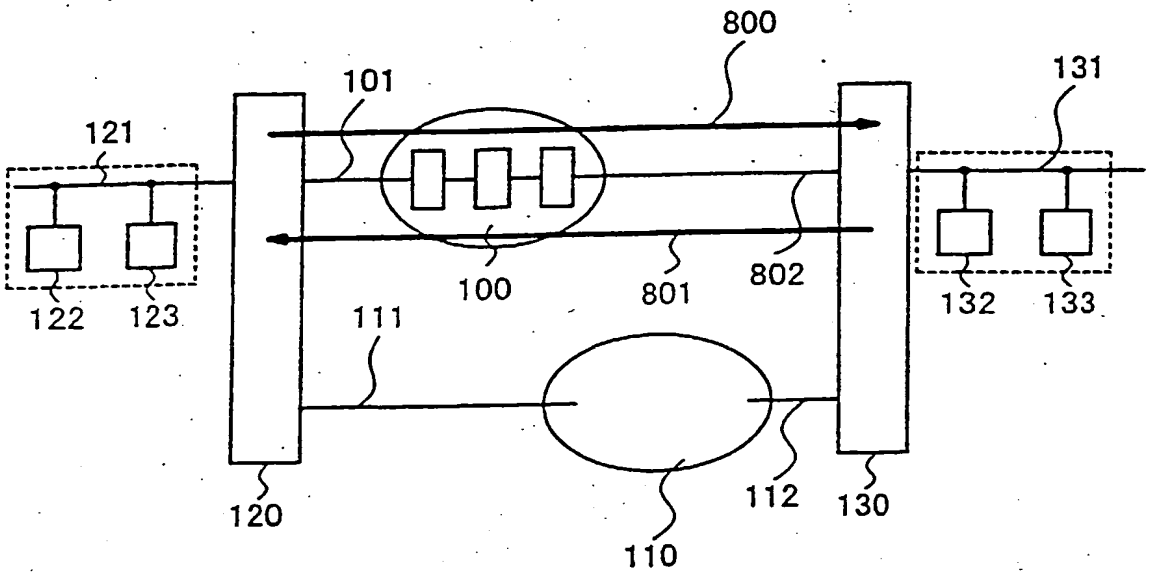
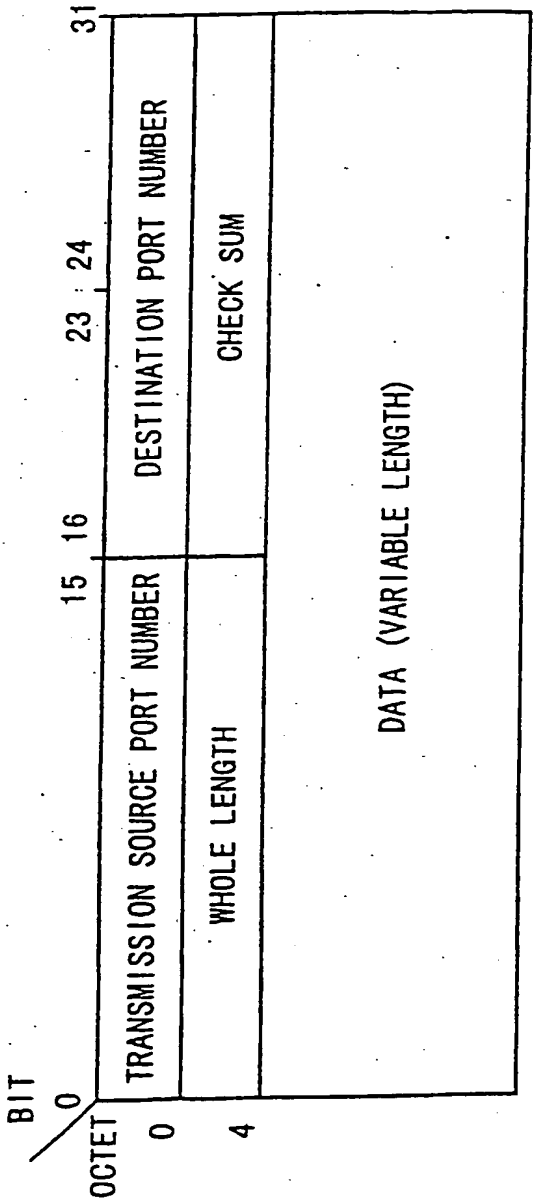


Fig. 9



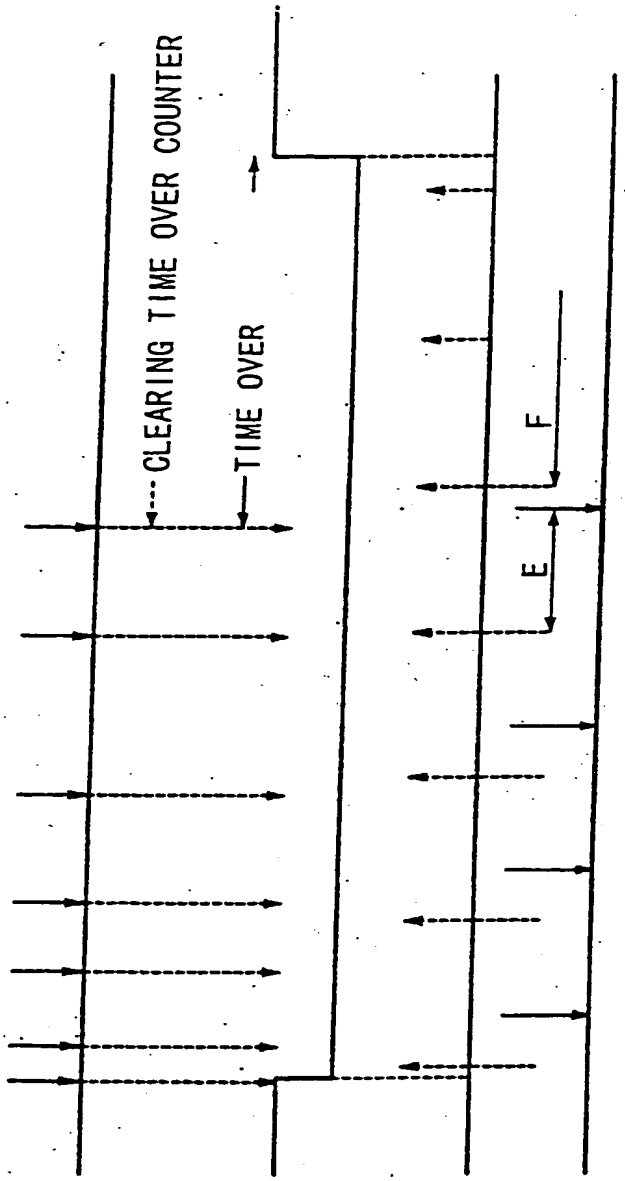


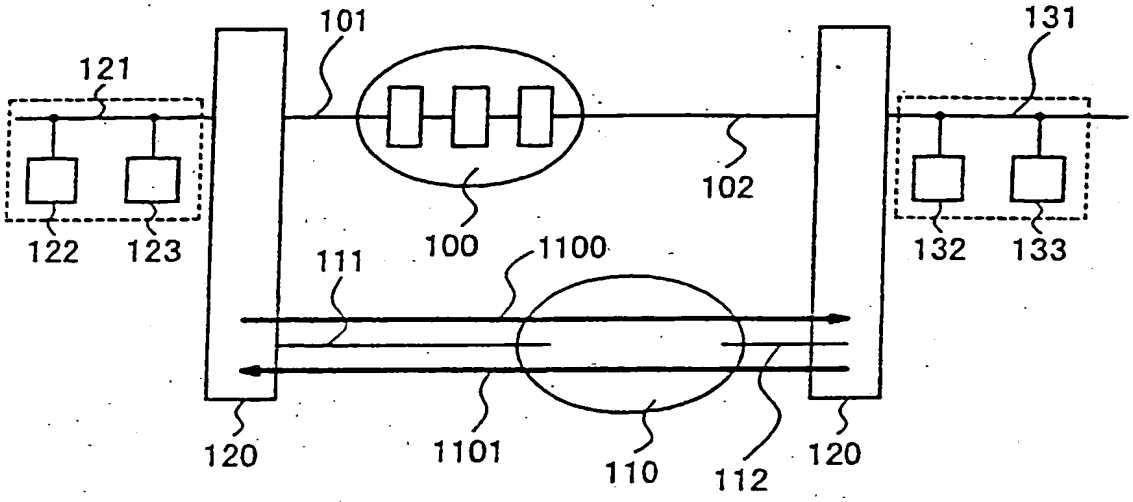
Fig. 10A

Fig. 10B

Fig. 10C

Fig. 10D

Fig. 11



METHOD FOR CARRYING OUT REAL-TIME BACKUP COMMUNICATION OF IP COMMUNICATION

Background of the Invention

1. Field of the Invention

The present invention relates to a method for carrying out real-time backup communication of Internet Protocol (referred to as "IP" hereinafter) communication. More particularly, the present invention relates to a method for carrying out real-time backup communication of IP communication using a public network.

2. Description of the Related Art

In recent years, real-time communication has begun to be used for data such as voice and animation of the Internet, Intranet and Extranet (hereafter referred to as "Internet network" or "IP network"). Activities of IETF standardization have become active with regard to the QoS (Quality of Security) control for securing the quality of real-time communication as much as possible. The main items among them are as follows:

(1) RSVP (ReSource reserVation Protocol): resource reservation protocol

(2) RTP (Real-time Transport Protocol)/RTCP (Real-time Transport Control Protocol): real-time communication control protocol

(3) DiffServe (Differentiated Service): priority

control using IP header

(4) RTSP (Real-time Transport Streaming Protocol): stream data Control Protocol

Those QoS controls alone can not carry out the real-time communication that is stable on the Internet network. For example, a real-time communication call such as voice data, animation data and the like, from a transmission side node causes an error at a reception side node because of troubles of a network and a node connected to the Internet network. A real-time communication that is communication in a UDP (User Datagram Protocol) procedure that does not carry out a re-transmission control does not have means for detecting the trouble of the Internet network on the node side. Thus, it is impossible to judge whether the trouble results from an opposite node trouble or a network trouble.

Under such situation, a maintenance technician having a high ability who firstly detects the network trouble based on a communication error report from a user uses a method for transmitting an echo request message between nodes, and firstly checking the error based on an absence of a reply with regard to an echo answer message, and manually switching to a public network such as INS and the like, to thereby carry out a backup switching operation. The specification of the trouble cause necessary for the execution of this

method requires high maintenance skill of the maintenance technician. Moreover, the maintenance technician having such high skill needs to carry out a large number of processes to specify the network trouble and the communication trouble. Moreover, it takes a long time to carry out a series of trouble analyses, from the user request to the manual operations, by the maintenance technician having the high maintenance skill, resulting in a large drop of related services.

Particularly associated with the down-sizing and flatting (horizontalizing) of the network resulting from the IP network in recent years, it is economically difficult to station the maintainers having the special and high skills for many respective small networks existing in an enterprise. So, a system begins to be required in which even a maintainer holding another low typical service, namely, an amateurish maintainer assigned in each department, can quickly specify the trouble reasons. In other words, the desire to establish a mechanism for economically insuring a reliability of the IP network has become popular in which the drop of the communication quality caused by the network trouble and the network delay time in the Internet network that is very economic, although being low in reliability and quality, can be monitored on a user-

equipment side by using a cheap method, and it is possible to carry out a stable continuous communication of a real-time communication call.

A related technique is disclosed in Japanese Laid-Open Patent Application (JP-A-Heisei, 10-224408) as "COMMUNICATION SYSTEM". First and second communication apparatuses in this communication system have switching means, data-format converting means and switching control means. The switching means contains a plurality of communication lines including a call path highway provided with a plurality of channels, which are connected to public networks, dedicated lines and inner terminals. The data format converting means connects a computer network and the call path highway, and converts a format of a transmission data between the computer network and the call path highway, and also transmits and receives data to and from a destination communication apparatus through the computer network. The switching control means transmits and receives call control information to and from the destination communication apparatus through the computer network, and also controls the switching means and the data format converting means so as to establish the connection using the computer network, in accordance with the data kinds at a terminal on a transmission side and a terminal on a reception destination. According to this

communication system, a mutual communication can be done between the terminals, in which the data kinds are different from each other, by using the computer network without a manual operation.

Japanese Laid-Open Patent Application (JP-A-Heisei, 10-65737) discloses "SUBSTITUTE SERVER APPARATUS AND SERVER APPARATUS". The substitute server apparatus contains: means for carrying out a PPP connection through a public network between a network and the server apparatus, by dynamically assigning an IP address in accordance with a specified server apparatus name and a telephone number in a corresponding public network, between the network and the server apparatus; and means for accessing the server apparatus by using the dynamically-assigned IP address. Accordingly, with regard to the server apparatus to be connected to the network managed by the IP address through the public network, even if it is not connected to the network at a time of the communication request, and if even further the IP address is not determined, it is possible to connect the server apparatus to the network and dynamically assign the IP address and further communicate with the dynamically-assigned IP address based on the server apparatus name.

Moreover, Japanese Laid-Open Patent Application (JP-A-Heisei, 9-130429) discloses "COMMUNICATION SYSTEM". In this communication system, a line/packet

converter is connected between a computer network and a call path highway in a private switch. A computer terminal transmits and receives a call control packet to and from the private switch through the computer network. The line/packet converter converts a format of a transmission data between the computer network and the call path highway. Accordingly, it is possible to connect the computer network, a subscriber line, and an extension line so that the computer terminal can communicate with another communication terminal through a public network and an extension line network.

Summary of the Invention

Therefore, an object of the preferred embodiment of the present invention is to provide a method for carrying out real-time backup communication of IP communication, which can protect a drop in communication quality caused by network delay time and network trouble in an Internet network that is very economic, by using a cheap and simple method.

Another object of the preferred embodiment of the present invention is to provide a method for carrying out real-time backup communication of IP communication, which can attain a technique for economically insuring a reliability of an Internet network by executing real-time communication stably and continuously.

Means for solving the above-mentioned problems are explained as follows. A number, a symbol or the like, together with parentheses "()", is given to a technical item appearing in the explanation. The number, the symbol or the like coincides with a reference number, a reference symbol or the like given to a technical item constituting at least one embodiment or a example among a plurality of embodiments or a plurality of examples in the present invention, especially a technical item illustrated in a drawing corresponding to the embodiment or the example. Such reference numbers and reference symbols evidently denote a corresponding relation between the technical item noted in the claims and the technical item in the embodiment or the example. Such corresponding relation does not imply the interpretation that the technical item noted in the claims is not limited to the technical item in the embodiment or the example.

A method for carrying out a real-time backup communication of IP communication according to the present invention comprises a step of detecting an occurrence of trouble in a real-time communication on an IP network (100) connecting between a transmission-side node (120) and a reception-side node (130), and a step of automatically bypassing a communication call of the real-time communication

performed between the transmission side node (120) and the reception side node (130), from the IP network to a public network (110), based on the detection. Such a bypass operation enables the continuation of the real-time communication. The occurrence implies a generation of a delay time to the extent that the quality of the real-time communication can not be secured. ICMP is used for the periodical transmission and reception.

There may be a case that a real-time communication call is newly-generated during the course of the real-time communication. In this case, the bypass operation of the new real-time communication call to the public network (110) is performed to thereby enable the real-time communication. If the trouble is recovered, the real-time communication is returned from the public network back to the IP network.

There may be a case that the trouble is induced even in the public network. During the bypass operation, the occurrence of the trouble is detected in the real-time communication on the public network connecting between the transmission-side node and the reception-side node. The detection is executed by detecting a time in the periodical transmission and reception with regard to an echo request message and an echo answer message between the transmission-side

node (120) and the reception-side node (130). In the detection during the bypass operation, if the echo request message is normally received while the trouble is induced on the public network (110), it is judged that the public network (110) is normal and the node (120 or 130) is abnormal.

The detection on the IP network (100) is executed by detecting the time of the periodical transmission and reception with regard to the echo request message and the echo answer message between the transmission-side node (120) and the reception-side node (130). In the detection, if the echo answer message is normally replied, it is judged that the IP network (100) has no trouble and the node (120 or 130) has a trouble. Typically, the discrimination between the trouble in the node (120, 130) and the trouble on the IP network (100) can be done by detecting the recovery of the trouble on the IP network (100) and detecting the occurrence of the trouble in the real-time communication on the public network (110).

Brief Description of the Drawings

Preferred features of the present invention will now be described, by way of example only, with reference to the accompanying drawings, in which:-

Fig. 1 shows a circuit block diagram used in an embodiment of a method for carrying out a real-time backup communication of IP communication according to the present invention;

Fig. 2 shows a data configuration of Ethernet

Frame with Tag of IEEE 802.1Q;

Fig. 3 shows a time chart representing a method for controlling RSVP;

Fig. 4 shows a data configuration indicating a field format with regard to a priority control in a conventional technique and the present invention;

Fig. 5 shows an IP datagram format and function;

Fig. 6 shows a kind of ICMP message;

Fig. 7 shows an echo answer message and an echo request message format in ICMP;

Fig. 8 is a circuit block diagram showing a part of operation signals of Fig. 1;

Fig. 9 shows a data configuration indicating a message format of UDP;

Figs. 10A to 10D show a timing chart of a signal flow of detecting a delay of an answer; and,

Fig. 11 shows a circuit block diagram of a well-known apparatus.

Description of the Preferred Embodiments

Coinciding with and corresponding to the drawings, in an embodiment of a method for carrying out a real-time backup communication of IP communication according to the present invention, a public (line) network 110 is provided together with an IP network 100. As shown in Fig. 1, a transmission side node 120 is connected through an IP-side first

connection interface 101 to the IP network 100. The IP network 100 is connected through an IP-side second connection interface 102 and an IP-side third connection interface 103 to a reception-side first node 130 and a reception-side second node 140, respectively.

The transmission-side node 120 is connected through a public-network-side first connection interface 111 to the public network 110. The public network 110 is connected through a public-network-side second connection interface 112 and a public-network-side third connection interface 113 to the reception-side first node 130 and the reception-side second node 140, respectively.

A transmission-side voice terminal 122 and a transmission-side animation terminal 123 are connected to a transmission-side LAN 121. The transmission-side LAN 121 is connected to the transmission-side node 120. A first reception-side voice terminal 132 and a first reception-side animation terminal 133 are connected to a first reception-side LAN 131. The reception-side LAN 131 is connected to the reception-side first node 130. A second reception-side voice terminal 142 and a second reception-side animation terminal 143 are connected to a second reception-side LAN 141. The second reception-side LAN 141 is connected to the reception-side second node 140.

In the real-time communication such as a multi-media communication in which voice data and animation data are transmitted and received, TCP (Transmission Control Protocol) is not used, because the TCP brings about a delay by a message re-transmission when a communication error is induced. The TCP is defined by setting a *protocol field (refer to Fig. 5) to "06" in Hexadecimal Number. Then, UDP (User Datagram Protocol) is used, because the UDP does not bring about the re-transmission even if an error is induced. The UDP is defined by setting a *protocol field (refer to Fig. 5) to "17" in Hexadecimal Number.

The voice terminal 122 and the animation terminal 123 which are connected to the LAN 121 are operated in accordance with "Ethernet Frame with Tag of IEEE 802.1Q" shown in Fig. 2. When the voice and animation having a high real-time property is transferred, a three-bit User Priority field formed in a Tag field of this Ethernet Frame is set to a value having the highest priority.

The IP network 100 has the configuration to enable the controls such as RSVP (ReSource reserVation Protocol) shown in Fig. 3, DiffServe (Differentiated Services), a QoS setting at IP over ATM, and the like. In a section "A" of Fig. 3, a resource reservation message is periodically sent out and a securing of resources is continued. RSVP is used for a control,

e.g. a signaling control for interpolating a network layer (IP), to enable QoS (Band Security) for a voice and animation having a high real-time property and is a protocol to reserve a network resource in a single direction under an instruction on a reception side for receiving information. DiffServe is a priority control service based on a contract between a user and an ISP (Internet Service Provider). To realize a priority control by using IP header, a TOS (Type Of Service) field (8-bit length) in an IP header which is shown in Fig. 4 and was not almost used, is again defined as a Differentiated Services field. The higher 6 bits of the Differentiated Services field is named as a PHB (Per-Hop-Behavior) field and three bits among the higher 6 bits can be used to set a six-level priority.

Moreover, the IP network 100 is provided with an RTP/RTCP (Real-time Transport Protocol / Real-time Transport Control Protocol) and an RTSP (Real-time Transport Streaming Protocol). The RTP/RTCP is a real-time communication control protocol for carrying out a synchronous control between media and a control of a reproduction speed on a reception side, by giving a sequence number and physical time information for each message to a header from a transmission-side terminal, in order to improve real-time communication quality between the terminals, namely, between an application

and a transport layer, independently of a network. Also, the RTSP (Real-time Transport Streaming Protocol) is a stream data control protocol for dynamically informing a communication speed and a display quality, such as a resolution and a number of animation frames per second from the reception side, to the transmission side.

It may be considered that a real-time telephone communication is done between the transmission-side voice terminal 122 on the LAN 121 and the first reception-side voice terminal 132 on the first reception-side LAN 131, through the IP network 100. The transmission-side voice terminal 122 sets DA (Destination Address) corresponding to the first reception-side voice terminal 132 for "Ethernet Frame with IEEE 802.1Q Tag" shown in Fig. 2, and sets the highest priority bit in the User Priority field of the Tag, and then transmits to the transmission-side node 120.

The transmission-side node 120 converts the DA (Destination Address) on the transmission-side LAN 121 into an IP number (IP number of the reception-side first node 130) corresponding to the first reception-side voice terminal 132, and simultaneously detects the highest priority bit in the User Priority field, and then maps to the QoS control (RSVP, DiffServe or IP over ATM) of the IP network 100.

As an example, a case is described in which the transmission-side node 120 sets the highest priority bit to the three bits in the PHB field of the IP header in the DiffServe of Fig. 4 and then transmits to the IP network as the QoS control. As a result, as shown in Fig. 1, it is possible to reserve the real-time communication in which the QoS is reserved up to the transmission-side voice terminal 122 - the transmission-side LAN 121 - the transmission-side node 120 - the IP-side first connection interface 101 - the IP network 100 - the IP-side second connection interface 102 - the reception-side first node 130. Moreover, the reception-side first node 130 sets the highest-priority bit to the User Priority field in the Tag and the DA corresponding to the first reception-side voice terminal 132 into "Ethernet Frame with 802.1Q Tag" shown in Fig. 2, and transmits it from the internal LAN 131 to the first reception-side voice terminal 132. Thus, it is possible to attain the real-time communication based on the QoS control through the IP network 100 between the transmission-side voice terminal 122 and the first reception-side voice terminal 132.

If 8 bits in a *protocol shown in Fig. 5 is "01" in Hexadecimal Number, ICMP (Internet Control Message Protocol) is specified as shown in Figs. 6 and 7. If 8 bits of "type" shown in Figs. 6 and 7, which

represents a message type, are "08" in Hexadecimal Number, this indicates an echo request, and if "00", this indicates an echo answer. An echo function including the echo request and the echo answer is used when it is checked whether or not a host or a node connected to the IP network 100 is active. Thus, if a certain host or node transmits an echo request of a message type "08", a specified host or node repeats an echo answer of a message type "00", when it is in the state which can respond. The operational check using such an echo is frequently done. The echo request is transmitted by using a utility program typically referred to as a ping.

As shown in Fig. 8, the transmission-side node 120 sets an IP address number of the transmission-side node 120 to a transmission-source address field shown in Fig. 5, sets an IP address number of the node 130 into a destination address field, sets "01" in Hexadecimal Number (ICMP) to the *protocol, and further sets "08" in Hexadecimal Number (the echo request shown in Fig. 6) to the message-type field shown in Fig. 7, and then transmits an echo request message 800 of Fig. 8, in which a test data for a loop back is set to a data (variable-length) field of Fig. 7, through the IP network 100 to the reception-side first node 130.

The reception-side first node 130, when

receiving the echo request message 800 of Fig. 8, sets the IP address number of the reception-side first node 130 into the transmission-source address field of Fig. 5, sets the IP address number of the transmission-side node 120 into the destination address field, sets "01" in Hexadecimal Number (ICMP) into the *protocol field, and further sets "00" in Hexadecimal Number (the echo answer of Fig. 6) into the message-type field of Fig. 7, and copies the test data for a loop back, which is written to a data field of the received echo request message 800 of Fig 8, to the data field (the variable length) in its original state, and then sends back to the transmission-side node 120 as an echo answer message 801 of Fig. 8. Thus, the transmission-side node 120 that is the transmission-source node can check the state of the transmission and reception of the data through the loop back test and also detect the troubles of a network and a node on a route in the transmission-side node 120 - the IP-side first connection interface 101 - the IP network 100 - the IP-side second connection interface 102 - the reception-side first node 130. Simultaneously, the transmission-side node 120 can check that the excellent quality of the real time telephone communication can be reserved if a round trip time until the reception of the echo answer message 801, sent back from the reception-side first node 130 after the transmission-side node 120

transmits the echo request message 800, is within a time capable of reserving quality of a real-time communication, for example, if it is within 150 msec defined by ITU-TG.114.

Under such precise conditions, when the transmission-side voice terminal 122 shown in Fig. 1 carries out the real-time communication with the first reception-side voice terminal 132 through the transmission-side LAN 121, the transmission-side node 120, the IP-side first connection interface 101, the IP network 100, the IP-side second connection interface 102, the reception-side first node 130 and the first reception-side LAN 131, the transmission-side node 120 receives the Ethernet frame with the Tag shown in Fig. 2 coming from the transmission-side LAN 121. Then, the highest priority detection of the QoS is done in accordance with the User Priority within the Tag. Accordingly, a conversion from the DA into the IP address number of the first reception-side voice terminal 132 is executed.

At the same time, as shown in Fig. 10A, a voice data packet coming from the transmission-side LAN 121 to the transmission-side node 120 causes a time-over counter for detecting a voice data packet disconnection shown in Fig. 10B to be cleared, and it is switched to a voice communication mode (L level). Here, Fig. 10A shows the voice data packet between the

voice terminal 122 → the LAN 121 → the node 120 in case of the real-time communication to the voice terminal 132 from the voice terminal 122. Also, Fig. 10B shows an output of the time over counter for a voice data packet disconnection detection between LAN 121 → node 120 (L level represents voice communication, H level represents non-voice communication).

After that, in order to reserve the real-time communication from the transmission-side LAN 121 to the transmission-side node 120, the time-over counter is cleared for each voice data packet, which always comes within a certain succeeding time, and the voice communication mode (L level) is continued.

Associated with the end of the voice communication, since the signal to clear the time-over counter does not issue, the time-over counter causes the time-over. Therefore, it is switched to a non-call mode (H level). The transmission-side node 120 sets the highest priority bit for the three bits in the PHB field of the IP header in the DiffServe shown in Fig. 4 as the QoS control, sets "17" in Hexadecimal Number (UDP) to the *protocol field of Fig. 5, sets the IP address number of the transmission-side node 120 accommodating the transmission-side voice terminal 122 to the transmission-source address field, sets the IP address number of the reception-side first node 130

accommodating the first reception-side voice terminal 132 to the destination address field, and copies voice data at a payload in the Ethernet frame with IEEE 802.1Q Tag shown in Fig. 2 to the data field (variable portion) of the UDP in the transport layer of Fig. 9, and then transmits through the IP network 100 to the reception-side first node 130. The reception-side first node 130 transmits this received voice data to the first reception-side voice terminal 132, by detecting a real-time communication call, namely, the QoS control request call, in accordance with a destination port number of the UDP of Fig. 9, namely, an application, and the priority bit of three bits in the PHB in the IP header of Fig. 4, and then setting the highest priority bit in the User Priority field in the Ethernet frame with IEEE 802.1Q Tag of Fig. 2 on the first reception-side LAN 131. As a result, the real-time communication securing the QoS can be done between the transmission-side voice terminal 122 and the first reception-side voice terminal 132.

At the same time, the transmission-side node 120, as the QoS control, sets the highest priority bit for the three bits in the PHB field of the IP header in the DiffServe of Fig. 4, sets "01" in Hexadecimal Number (ICMP) to the *protocol field of Fig. 5, sets the IP address number of the transmission-side voice

terminal 122 to the transmission-source address field, sets the IP address number of the first reception-side voice terminal 132 (the IP address number of the reception side first node 130) to the destination address field, sets "08" in Hexadecimal Number (echo request) to the message-type field of Fig. 7, and transmits the echo request message 800 of Fig. 8, in which the test data for loop back is set for the data field (variable length), through the IP network 100 to the reception-side first node 130.

After that, this echo request message 800 is periodically transmitted for each constant interval (period) shown in Fig. 10C, in the voice communication mode at which an output from the time-over counter is at the L level. Here, Fig. 10C represents a sending-out time range and a sending-out interval of the echo request message 800 of Fig. 8 in ICMP. The transmission-side node 120 detects whether or not the round trip time until the reception of the echo answer message 801 sent back from the reception-side first node 130 within the constant time in Fig. 10C is within a time in which the quality of the real-time communication can be reserved, by using the time-over counter shown in Fig. 10D. Here, Fig. 10D represents a delay time from the transmitting of Fig. 10C to the reception of the echo response message 801 of Fig. 8. In Fig. 10D, "E" represents a case of the occurrence

of the time over because the delay time from the transmitting of Fig. 10C to the reception of the echo response message 801 is large, and "F" represents a case of the occurrence of the time over because of being not received the echo response message 801. Then, it judges that the trouble results from the IP or the opposite node 130, if the echo answer message 801 after an elapse of the round trip time is not received as shown in E of Fig. 10D and if the echo answer message 801 is not replied as shown in F of Fig. 10D.

In this case, the transmission-side node 120 converts the IP address number of the first reception-side voice terminal 132 at the connection destination (the IP address number of the reception side first node 130) into a telephone number of the public network 110, and then reserves a backup bypass route up to the transmission-side node 120 - the public-network-side first connection interface 111 - the public network 110 - the public-network-side second connection interface 112 - the reception-side first node 130, through the public network connection based on a dialup. The transmission-side node 120 transmits an echo request message 1100 of Fig. 11 through the public network 110 after the backup-switch bypass operation, to the reception-side first node 130, and then judges that the IP network 100 is abnormal and

the reception-side first node 130 is normal if the echo answer message 1101 from the reception-side first node 130 is replied within an allowable time, and judges that the reception-side first node 130 is abnormal if the echo answer message 1101 is not replied. So, it can request an emergent treatment if detecting the trouble in the reception-side first node 130.

Moreover, in order to continuously monitor the normal conditions with regard to the reception-side first node 130 and the public network 110 through the communication route of the public network 110 during the real-time communication resulting from this backup bypass operation, this is designed such that the operations perfectly equal to those in the series of configurations shown in Figs. 8, 10 are also applied to a public network 110 in Fig. 11, namely, the echo request message 800 is replaced by an echo request message 1100 of Fig. 11, and the echo answer message 801 is replaced by an echo answer message 1101 of Fig. 11.

At the same time, the transmission-side node 120, in order to monitor the normal recovery from the network congestion, in which the IP delay time caused by the IP network disconnection/abnormal trouble and the round trip time-over is equal to or longer than a specified time, changes the condition shown in Fig.

10B into the IP trouble (including the round trip time-over) condition between the transmission-side node 120 and the reception-side first node 130, namely, a condition that Fig. 10B is forcedly switched to the L level at the time of the network trouble, and periodically transmits the echo request message 800 for each constant interval (period) shown in Fig. 10C.

The transmission-side node 120, after the transmission of the echo request message 800 of Fig. 8, namely, Fig. 10C, detects whether or not the round trip time until the reception of the echo answer message 801 sent back from the reception-side first node 130 within the constant time is within the time in which the quality of the real-time communication can be reserved, by using the time-over counter in Fig. 10D, and then continues to receive the echo answer message 801 after an elapse of an allowable limit time of the round trip time as shown in E of Fig. 10D or monitor until the recovery of the continuously (stably) normal state after the current trouble condition that the echo answer message 801 is not replied as shown in F of Fig. 10D. That is, this implies the continuation of the monitor until the IP network 100 between the transmission-side node 120 and the reception-side first node 130 recovers the normal state, even after the completion of the communication through the backup bypass operation between the

transmission-side node 120 and the reception-side first node 130. The backup bypass operation through the public network 110 is done if a communication call to the reception-side first node 130 is newly-generated during the continuous monitor.

After the check of the recovery of the normally-stable state in the IP network 100, if the real-time communication is done through the public network 110 from the transmission-side node 120 to the reception-side first node 130, switching to the IP network 100 whose normal state is recovered enables the communication to be done further economically. In this case, when the recovery to the normally-stable state is detected, the IP trouble condition in Fig. 10B, namely, the forced L level condition in Fig. 10B implying the network trouble state is once cleared and returned back to the H level implying the initial state. So, at a time of a start of the communication call to the IP, the monitor of the trouble in the IP network 100 is designed to be done in accordance with a normal sequence from Fig. 10A. It is also natural that the switching from the public network 110 to the IP network 100 is quickly done when the IP network 100 recovers the normal state, and then the series of typical real-time communications is done through the IP network 100, as mentioned above.

In the above-mentioned embodiment, it is

described that the transmission-side node 120 is used as the calling side and the reception-side first node 130 is used as the called side. However, if the transmission-side node 120 is used as the called side and the reception-side first node 130 is used as the calling side, the transmission-side node 120 can know that the reception call is the real-time communication call, from the port number of the UDP, namely, the application number, or the highest priority setting of the DiffServe priority bit in the PHB field in the IP header of Fig. 4. So, the execution of the operations perfectly equal to the series of operations in Figs. 10A to 10D and the series of operations in the echo request message 1100 and the echo answer message 1101 with regard to Fig. 11 enables the monitor of the IP trouble having the symmetry between the nodes, the monitor of the allowable delay time, the quick detection of the trouble and the maintenance.

In the above-mentioned explanation, the IP is described as the Internet network, for the purpose of easy explanation. However, it can include the intra-network and the extra-network. The real-time communication in the IP in which the QoS is secured is described in the above-mentioned explanation. However, it is possible to configure by using the currently-popular IP (Internet) network that is the best effort in which the QoS is not secured. So, the delay time

is monitored by monitoring the round trip time. Then, if it exceeds the limit time, the backup bypass operation to the public network is done to thereby enable the real-time communication to be further economically done.

In addition to the above-mentioned basic operations, MP (The PPP Multilink Protocol) is effective in order to reserve the stable quality of the communication that is easy and smooth, by solving the delay time and the packet loss in the real-time communication call induced in the backup switching or returning back operation when the trouble is induced in the IP (Internet) network 100, and then the normal state is recovered.

In the method for carrying out a real-time backup communication of IP communication according to the present invention, if the IP trouble is induced and the delay time is induced to the extent that the quality of the real-time communication can not be secured, it is treated as the real-time communication trouble, and the backup switching bypass operation can be automatically done to the public network 110. Moreover, in addition to the economically-large effect of enabling the real-time communication that is stable and high in quality on the very economical IP, although it is low in reliability and quality. So, this method can provide the largely economical effect that even a

low-grade maintainer, namely, a maintainer holding another typical service can carry out the maintenance operation without stationing a maintainer having high skill, and can quickly specify the trouble point and reduce the recovery time. Thus, it can improve the quality of the communication service and obtain the economical effect.

While the present invention has been described in its preferred embodiments, it is to be understood that the words which have been used are words of description rather than limitation, and that changes may be made to the invention without departing from its scope as defined by the appended claims.

Each feature disclosed in this specification (which term includes the claims) and/or shown in the drawings may be incorporated in the invention independently of other disclosed and/or illustrated features.

The text of the abstract filed herewith is repeated here as part of the specification.

A method for detecting an occurrence of trouble in a real-time communication on an IP network through which a transmission-side node and a reception-side node are connected, and automatically bypassing a communication call of the real-time communication performed between the transmission-side node and the reception-side node from an IP network to a public network, based on the detecting result. Such a bypass operation enables the continuation of the real-

time communication. The occurrence of the trouble implies an occurrence of a delay time to an extent that the quality of the real-time communication can not be secured. ICMP is used in a periodical transmission reception. There may be a case that the real-time communication call is newly-generated during the course of the real-time communication on the public network. In such a case, this makes even the new real-time communication go around the public network to thereby enable the real-time communication. If the trouble is recovered, the real-time communication is returned from the public network to the IP network. Thus, it is possible to avoid a drop of communication quality, caused by the network delay time and the network trouble in the economical Internet network, by using a cheap and simple method.

CLAIMS:

1. A method for carrying out a real-time backup communication of Internet Protocol (IP) communication, said method comprising the steps of:

detecting when the duration of a delay time, extending from transmission of an echo request message from a transmission side node to reception of an echo answer message at a reception-side node, exceeds a predetermined allowed time interval indicative of secured quality of a real-time communication on an IP network;

bypassing, depending on a result of the detecting step, from said IP network to a public network, a communication call of said real-time communication performed between said transmission-side node and said reception-side node; and,

bypassing a new communication call that occurs while said bypassing operation of said communication call to said public network is being performed.

2. A method according to claim 1, further comprising the step of judging, after the detected duration of the delay time has exceeded the predetermined allowed time, whether said IP network or said reception-side node is abnormal.

3. A method according to claim 1, further comprising the step of detecting an error in a real-time communication on said public network through which said transmission-side

node and said reception-side node are connected, said further step comprising detecting, on said public network, a duration of a delay time from a transmission of an echo request message to a reception of an echo answer message between said transmission-side node and said reception-side node.

4. A method according to claim 1, further comprising the step of detecting an error in a real-time communication on said public network through which said transmission-side node and said reception-side node are connected, said further step comprising judging, after the detected duration of a delay time for response to an echo request message has exceeded a predetermined allowed time interval for response to said message, whether said public network is abnormal.

5. A method according to claim 4, further comprising the step of judging after said public network has been found to be normal, whether it is the reception-side node that is abnormal or the IP network that is abnormal, the judgment being based on measuring the delay time for an echo signal passed along the public network after the communication call has been bypassed to the public network from the IP network.

6. A method according to any one of the preceding claims, wherein Internet Control Message Protocol (ICMP) is used in said transmission of said echo request message and reception

of said echo answer message.

7. A system configured to effect the method of any one of claims 1 to 6.

8. A method for carrying out a real-time backup communication that includes one step of bypassing a communication call from an IP network to a public network and another step of bypassing a new communication call while the one step is being performed, the method being substantially as herein described with reference to, and as shown in, Figures 1 to 10 of the accompanying drawings.

Application No: GB 0202535.1
Claims searched: 1-8

Examiner: John Cullen
Date of search: 27 February 2002

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.T): H4P (PPD, PEE, PENE, PENX, PEX)

Int Cl (Ed.7): H04L 1/12, 1/14, 1/20, 1/22, 12/66, 29/06; H04M 7/00, 3/22, 3/42

Other: WPI, EPODOC, JAPIO

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
A, E	EP 1035719 A2	(SIEMENS) See entire document.	---
A	EP 0920176 A2	(NORTHERN TELECOM) See Abstract, Fig. 1 and line 36 of col. 2 to line 37 of col. 3.	---
A	EP 0910201 A2 (ALCATEL) See Figs. 1 and 2, paragraphs 9 to 13, claims 1 and 3, and also WPI Abstract Accession No. 1999-231838/20.		---
A	WO 99/28979 A2	(ALCATEL) See lines 1-10 of page 15	---
A	US 5898668	(SIEMENS) See entire document.	---
A	JP 110308345	(NEC) See Abstract	---

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

BNSDOCID: <GB___2369019A__I_>